The global problem of image-based sexual abuse considered in the Irish context: An evaluation of existing legal responses with a focus on effective enforcement in the online environment

Emer Shannon

Student Number: 12401732

Qualification: Doctor of Philosophy (PhD) in Law

Institution: Maynooth University Department of Law

June 2023

Head of Department: Professor Michael Doherty

Supervisor: Dr Maria Helen Murphy

Acknowledgments

This thesis has graciously been funded by the Department of Law, Maynooth University Scholarship. I would like to express my deepest gratitude to the many people without whom this thesis would not have been completed.

I am grateful to the staff within the Department of Law at Maynooth University, for the many opportunities they granted me and for providing me with guidance and support. I am especially thankful to Professor Michael Doherty for his unending support. You have been instrumental in helping me along this academic journey.

I am also deeply grateful to all the research participants, who kindly volunteered their time and shared their knowledge and experience with me. This research would not have been possible without your valuable input.

I am especially thankful for my supervisor, Dr Maria Helen Murphy, for her unending patience, valuable comments, and feedback throughout. Thank you, Maria, for always shining a light and directing me towards the finish line. Thank you for your unwavering support, insightful advice, and generosity. Without your encouragement, guidance, and hard work I would never have been able to complete this research. I am eternally grateful.

I am lucky to have such an incredibly supportive family, who have been a consistent source of love. Thank you so much Mom, Dad, Orla, and Joseph.

A special word of thanks to my loving husband John who is hugely important to me and has kept me smiling through the highs and lows. Thank you for keeping me sane, for believing in me, and for always being there. No words can describe my love and gratitude.

Lastly, this thesis is dedicated to my granny Catherine Mulhern.

Plagiarism Declaration

I hereby certify that this material, which I now submit for assessment on the programme of study leading to the award of PhD in Law, is entirely my own work and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the text of my work.

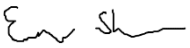
Signed:  **Date:** 21/05/23

Table of Contents

Table of Figures

Abbreviations

AVMSD	Audiovisual Media Services Directive
DSA	Digital Services Act
DMA	Digital Markets Act
DSC	Digital Safety Commissioner
IBA	Image-Based Abuse
IBSA	Image-Based Sexual Abuse
IHREC	Irish Human Rights and Equality Commission
ISPCC	Irish Society for the Prevention of Cruelty to Children
LRC	Law Reform Commission
OESC	Office of the eSafety Commissioner
OSC	Online Safety Commissioner

Abstract

The recording and/or sharing of intimate images without consent – known as image-based sexual abuse (IBSA) – has received significant legislative attention in recent years. Various approaches to addressing the harm of IBSA have been adopted internationally and this thesis identifies a need to consider the Irish response to IBSA. Adopting a victim-centred approach, this thesis derives lessons from the Australian experience where an innovative system of redress and enforcement has been developed through the establishment of a regulatory structure supported by a statutory body, the Office of the eSafety Commissioner (OESC). The immediate importance of this research is clear. Remediating harm in the world of the internet where both identities and jurisdictional boundaries are blurred is challenging. This thesis investigates the effectiveness of the OESC in practice in order to better assess the Irish approach and the potential of the Irish Online Safety Commissioner to provide adequate redress for victims of IBSA in Ireland.

Through the use of doctrinal and comparative analysis and the conducting of interviews with key stakeholders in the area of online regulation, this thesis identifies the key needs of victims of IBSA and identifies numerous mechanisms designed to address those needs, at least in part. This victim-centred approach underlies the in-depth analysis of the Australian system and is used to inform the policy recommendations made in this thesis. Particular attention is afforded to whether the Irish approach should include an individual complaints mechanism. By drawing inferences between the Irish and Australian situations, a clearer picture is drawn as to the optimum remit, structure, functions, and powers of the Irish OSC in order to effectively address the harms of IBSA.

Introduction

(1) Context

As technology and social media increasingly infiltrate daily life, the recording and/or sharing of intimate images without consent – known as image-based sexual abuse (IBSA) – has become a significant phenomenon demanding legislative action. Once an image is shared online without consent, the victim faces significant harm and loss of autonomy over their own image. A person's most intimate moments can be exposed and displayed online for users around the world to view, share, and download. Among those viewing such images may be employers, family members, and social contacts. While the concept of IBSA is not a new phenomenon, its spread has been adapted and facilitated by advances in technology and the evolution of relationships in the 21st century. Globally, IBSA has been the subject of much debate and the target of many legislative measures.[1] Adopting a victim-centred perspective, this thesis examines the Irish legislative response to the harm of IBSA and offers recommendations on how to best improve the response. These recommendations are informed by lessons learned from the Australian response to IBSA, with a particular focus on the development and operation of the Australian online safety regulatory system as supported by the Office of the eSafety Commissioner (OESC). In order to achieve these goals, it is necessary to understand the harms that IBSA can cause, to investigate the needs of IBSA victims, and to consider how the needs of IBSA victims can be best met through law and policy. Determining the suitability of existing and proposed tools/mechanisms to address these needs is part of this assessment.

It is increasingly accepted that IBSA should be a criminal offence with many jurisdictions implementing targeted legislation criminalising the act of sharing intimate images without consent.[2] IBSA was criminalised in Ireland in late 2020 under the Harassment, Harmful Communications and Related Offences Act. In spite of this progress, the criminalisation of IBSA alone is insufficient in adequately addressing the harms of IBSA and as a result there is significant momentum behind the development of regulatory mechanisms

[1] Mary Ann Franks, 'Drafting an Effective 'Revenge Porn' Law: A Guide for Legislators' (*Cyber Civil Rights Initiative*, 22 September 2016) 3 <https://www.cybercivilrights.org/wp-content/uploads/2016/09/Guide-for-Legislators-9.16.pdf> accessed 24 August 2022.

[2] Beginning in the late 2000s, several jurisdictions have implemented IBSA targeted laws including England and Wales, Scotland, Northern Ireland, Canada, Philippines, Israel, Japan, and 48 states in America. Mary Ann Franks, 'Drafting an Effective 'Revenge Porn' Law: A Guide for Legislators' (*Cyber Civil Rights Initiative*, 22 September 2016) <https://www.cybercivilrights.org/wp-content/uploads/2016/09/Guide-for-Legislators-9.16.pdf> accessed 24 August 2022.

designed to help tackle the challenges of IBSA. Of direct relevance to this thesis, the development of a regulatory system with responsibility in the area of IBSA has been a topic of consideration for numerous Irish governments since 2016.

In 2016 the Irish Law Reform Commission (LRC) released a report outlining the need for a state sanctioned regulatory body to pursue digital safety. The report proposed the establishment of a Digital Safety Commissioner (DSC) – modelled on the Australian Office of the eSafety Commissioner (OESC) – to enforce the removal of certain categories of online harmful content, with specific attention on IBSA material. In 2018, the Chairman of the Oireachtas Committee on Children and Youth Affairs and member of Fine Gael, Alan Farrell, stated that this body should be set up 'without delay'.[3] By 2019, the then Minister for Communications, Climate Action and Environment, Richard Bruton announced plans for the development of a different regulatory model, to be supported by the establishment of a new entity, an Online Safety Commissioner (OSC).[4] While the newly proposed system would have some key differences from the Australian system, the design of the OSC was still intended to be influenced by the Australian approach. On the 10th of December 2022, the Online Safety and Media Regulation Act (OSMRA) was enacted. The Act establishes Coimisiún na Meán as the Irish body with regulatory responsibilities for broadcasting, the Audiovisual Media Services Directive, and Online Safety. Provision is made in the OSMRA for the Commission to delegate certain functions to an Online Safety Commissioner. Key elements of the new regulatory system remain uncertain as Coimisiún na Meán must first draft binding Online Safety Codes and designate which online services fall under the purview of these codes.

As the new regulatory structure begins to take shape, enforcement challenges remain, and the debate on intermediary responsibility has been a key point of issue. Remediating harm in the distributed world of the internet where both identities and jurisdictional boundaries are blurred is challenging. Australia is a leading jurisdiction in advocating for the need for numerous enforcement responses and intermediary responsibility.[5] A nuanced

[3] Houses of the Oireachtas, Joint Committee on Children and Youth Affairs, *Report on Cyber Security for Children and Young Adults* (32 CYA 011 — March 2018).

[4] Department of the Environment, Climate and Communications, 'Minister Bruton Proposes New Law to Protect Children Online' (Government Press Release, 4 March 2019) < https://www.gov.ie/en/press-release/0799d6-minister-bruton-proposes-new-law-to-protect-children-online/ > accessed 8 September 2022.

[5] Law Reform Commission, Harmful Communications and Digital Safety (LRC 116 — 2016).

understanding of the highly influential Australian system is vital to make the best-informed assessment of the OSMRA and the regulatory system as it develops.

A core output of this thesis is to assess the effectiveness of the Australian OESC in practice from the perspective of key stakeholders who engage with this body. Learning from the perspectives of key stakeholders provides important practical insight and helps to fill gaps in understanding where published information is limited. An analysis of the powers and effectiveness of the Australian system and OESC using a victim-centred approach provides an informed basis from which to consider the potential effect of the new regulatory system and body in Ireland. By drawing inferences between the Irish and Australian situations, a clearer picture may be drawn as to what is best practice. There is the potential for Ireland to learn from the Australian approach and to adopt the elements of the system that have been successful in practice and improve upon the elements that have been less successful in achieving the goals of the legislation. This thesis provides an in-depth analysis of the Australian approach to IBSA, with a particular emphasis on the role of the Australian OESC, in order to inform the assessment of the regulatory approach in Ireland from a victim-centred perspective.

(2) Justification for use of the term 'image-based sexual abuse'

McGlynn and Rackley highlight how 'terminology frames debates and options for legal redress, as well as playing a vital expressive role'.[6] Furthermore, Henry and Powell highlight how poor use of terminology can not only be a 'deterrent to victims coming forward to report their experiences', but it may also 'shape problematic attitudes and beliefs' within society which may result in victim blaming attitudes and/or delays in changes to the law.[7] The first known term used to describe the recording and/or sharing of an intimate image or threat to do so without consent, was the media generated term 'revenge pornography' which was commonly associated with the leaking of private images by a vengeful ex-partner.[8] However, while this term resonated with the public, its

[6] Clare McGlynn & Erika Rackley, 'Image-Based Sexual Abuse' (2017) 37 Oxford Journal of Legal Studies 534.
[7] Nicola Henry, Asher Flynn & Anastasia Powell, 'Responding to 'Revenge Pornography': Prevalence, Nature and Impacts' Report to the Criminology Research Advisory Council Grant: CRG 08/15-16 (March 2019) 13.
[8] Nicola Henry, Clare McGlynn, Asher Flynn, Kelly Johnson, Anastasia Powell & Adrian J. Scott, '*Image-Based Sexual Abuse: A Study on the Causes and Consequences of Non-Consensual Nude or Sexual Imagery*' (1st edn, Routledge 2020); Nicola Henry & Asher Flynn, 'Image-based sexual abuse: Online Distribution Channels and Illicit Communities of Support' (2019) 25 Violence Against Women 1932.

use is problematic and has the been the subject of much critique on a number of intersecting bases. Citron and Franks highlight that the term 'revenge pornography' suggests that perpetrators are motivated only by personal vengeance whereas in reality perpetrators may have other motives, such as sexual gratification, monetary gain, social status building or a desire for power and control.[9] McGlynn, Rackley, Houghton, Powell, and Henry criticised the term 'revenge pornography' as being 'too narrow' and does not adequately capture the diverse behaviours such as upskirting, downblousing, or sextortion.[10] McGlynn and Rackley also critiqued this term describing it as 'skewing' the focus of legislative debates, with the language of 'pornography' leading some legislators to consider that regulation is dependent on an image being 'pornographic', or that the perpetrator must be acting for the purposes of sexual gratification.[11] Maddocks highlights that the term 'revenge pornography' has victim-blaming connotations as it implies that victims are to blame for causing or provoking perpetrators to seek revenge.[12]

The framing of language is 'powerful'.[13] In response to the many problems associated with the term 'revenge pornography', scholars have developed a range of other labels to describe the recording and/or sharing of intimate images or threatening to do so without consent. Such labels include 'non-consensual pornography',[14] 'involuntary porn',[15] 'nonconsensual sexting'[16] or 'image-based sexual abuse'.[17] In line with leading legal scholars in this field, this thesis uses the term 'image-based sexual abuse' because it

[9] Danielle Citron & Mary Ann Franks, 'Criminalizing Revenge Porn' (2014) 49 Wake Forest Law Review 345.
[10] Clare McGlynn & Erika Rackley, 'Image-Based Sexual Abuse' (2017) 37 Oxford Journal of Legal Studies 534; Clare McGlynn, Erika Rackley & Ruth Houghton, 'Beyond "Revenge Porn": The Continuum of Image-Based Sexual Abuse' (2017) 25(1) Feminist Legal Studies 256; Anastasia Powell & Nicola Henry, *'Sexual Violence in a Digital Age'* (1st edn, Palgrave Macmillan, London 2017).
[11] Clare McGlynn & Erika Rackley, 'Image-Based Sexual Abuse' (2017) 37 Oxford Journal of Legal Studies 534.
[12] Sophie Maddocks, 'From Non-consensual Pornography to Image-based Sexual Abuse: Charting the Course of a Problem with Many Names' (2018) 33 Australian Feminist Studies 345.
[13] Nicola Henry, Asher Flynn & Anastasia Powell, 'Responding to 'Revenge Pornography': Prevalence, Nature and Impacts' *Report to the Criminology Research Advisory Council Grant: CRG 08/15-16* (March 2019) 13.
[14] Danielle Citron & Mary Ann Franks, 'Criminalizing Revenge Porn' (2014) 49 Wake Forest Law Review 345.
[15] Anne Burns, 'In Full View: Involuntary Porn and the Postfeminist Rhetoric of Choice' in Claire Nally & Angela Smith (eds), *Twenty-First Century Feminism* (Palgrave Macmillan, London 2015).
[16] Nicola Henry & Anastasia Powell, 'Beyond the "Sext": Technology-Facilitated Sexual Violence and Harassment Against Adult Women' (2015) 48(1) Australian & New Zealand Journal of Criminology 104.
[17] Nicola Henry & Anastasia Powell, 'Beyond the "Sext": Technology-Facilitated Sexual Violence and Harassment Against Adult Women' (2015) 48(1) Australian & New Zealand Journal of Criminology 104; Clare McGlynn, Erika Rackley & Ruth Houghton, 'Beyond "Revenge Porn": The Continuum of Image-Based Sexual Abuse' (2017) 25(1) Feminist Legal Studies 256; Clare McGlynn, Erika Rackley, Kelly Johnson, Nicola Henry, Nicola Gavey, Asher Flynn, Anastasia Powell, Adrian Scott, 'Shattering Lives and Myths: A Report on Image-Based Sexual Abuse' (2019) *Project Report. Durham University; University of Kent.*

captures the broad array of behaviours and motivations, and also moves the focus to the abusive actions of those who misuse intimate imagery.[18] Furthermore, the use of the phrase 'sexual abuse' accurately conveys the significant harms that may occur and reflects the experiences of victim-survivors.[19]

(3) Research aims and questions

This thesis aims to conduct a comprehensive analysis of the Irish legislative approach to IBSA by considering the legislative history and drafting which led to the enactment of the OSMRA and analysing the potential of the nascent regulatory system for online safety to respond to the needs of victims of IBSA. In order to inform the victim-centred perspective of this thesis, academic literature and studies are examined and the Australian system is considered in depth. Overall, this thesis aims to establish the best means by which to tackle the harm of IBSA including by considering the most appropriate means to protect and remediate victims of IBSA. This has immediate policy relevance in Ireland but will also provide broader lessons that can be applied to other jurisdictions seeking to update their regulatory response.

The key research questions are as follows:

1. What are the key needs of IBSA victims?
2. What tools/mechanisms may be used to address the specific needs of IBSA victims?
3. What insights can be drawn from the Australian approach to IBSA?
4. How has the Irish policy and legal response to IBSA developed over time?
5. Applying lessons from Australia, what are the merits and demerits of the regulatory response in Ireland from a victim-centred perspective and should an individual complaints mechanism be introduced?

[18] For example, see the work of: Nicola Henry & Anastasia Powell, 'Beyond the "Sext": Technology-Facilitated Sexual Violence and Harassment Against Adult Women' (2015) 48(1) Australian & New Zealand Journal of Criminology 104; Clare McGlynn, Erika Rackley & Ruth Houghton, 'Beyond "Revenge Porn": The Continuum of Image-Based Sexual Abuse' (2017) 25(1) Feminist Legal Studies 256; Clare McGlynn, Erika Rackley, Kelly Johnson, Nicola Henry, Nicola Gavey, Asher Flynn, Anastasia Powell, Adrian Scott, 'Shattering Lives and Myths: A Report on Image-Based Sexual Abuse' (2019) *Project Report. Durham University; University of Kent*.

[19] Clare McGlynn & Erika Rackley, 'Image-Based Sexual Abuse' (2017) 37 Oxford Journal of Legal Studies 534.

(4) Methodology and structure of thesis

A number of methodologies inform the approach taken in this thesis. The methodology and methods followed when designing and conducting the interviews are discussed in more detail in Chapter 3, but it is necessary at this point to provide a brief overview of the methodologies employed in this thesis.

Doctrinal analysis

A foundational part of this project is an exploration into the governing legislation of the Australian OESC (including both past and current legislation) and relevant Irish legislation and proposals. When considering the laws establishing or proposing the regulatory bodies, doctrinal analysis is used in identifying the structure, functions, and powers of both the Australian OESC and the Irish OSC. Furthermore, in order to investigate the need for a supplemental system of complaint for victims of IBSA, doctrinal analysis of the various targeted criminal laws is employed. The use of doctrinal analysis enables a clear and comprehensive understanding of the suitability of existing and proposed legal responses to combating IBSA in Australia and Ireland, allowing the researcher to provide recommendations on how the law can evolve to address remaining gaps in protection. The Irish proposals undergo an in-depth examination, allowing for the identification of merits, limitations, and gaps in existing and proposed Irish law on the issue of IBSA.

Law in context analysis

A 'law in context' approach is adopted to consider broader issues and perspectives. This is particularly important as the issue of IBSA has significant technological, societal, economic, and cultural implications. By considering these social and technological aspects and investigating the environment in which the law operates, this thesis can provide a comprehensive account of the Irish situation. The use of contextually informed materials will allow this project to better assess the options for tackling the harms of IBSA while appreciating the potential for politically-driven moral frenzy to adversely influence the objective assessment of the optimum course. The use of materials such as empirical studies on sexting, social media usage, and 'selfie' culture will provide insights necessary to ensure the research is responsive to issues on the ground.

Qualitative study – interviews

While scrutiny of the legislative framework of the OESC in Australia is important, a need was identified to obtain additional information on how the OESC had been operating in practice, particularly in relation to IBSA. A number of key stakeholders were identified as potential candidates for interview in order to gain insight from their experiences with the OESC. As discussed in more detail in Chapter 3, semi-structured interviews with 14 non-vulnerable professionals were conducted in order to establish their perception of the OESC effectiveness in combating harmful online content such as intimate images and the role of online intermediaries. Interviewees included representatives from non-governmental organisations, legal practice, academia, industry, and the OESC. Semi-structured interviews were deemed appropriate because they enable the design of predetermined questions and allow for divergence and opportunities to probe beyond original questions where appropriate. The different perspectives provide a better contextual understanding of how the OESC operates in practice and how it is viewed by key stakeholders.

Comparative analysis

Bhat describes comparative analysis as a 'logical and inductive method of reasoning that enables objective identification of the merits and demerits of any norm, practice, system, procedure, or institution as compared to those of others'.[20] Furthermore, Jansen states the 'search for common or dissimilar properties is the essence of comparison'.[21] A crucial aspect of this thesis is to understand how Ireland can best respond to the challenge of IBSA, including by considering the potential role for a new regulatory system supported by a statutory authority. A key method to achieve this goal is to conduct an assessment of an already established approach to the same problem so to identify its merits and limitations in order to inform the Irish approach. As part of the analysis of the Australian system, it is necessary to closely examine the background and political context to the Australian laws and development of the OESC and take into account that 'the goals of law can be achieved by different rules and institutions in different social contexts'.[22]

The selection of laws, countries, or legal systems for comparison is a crucial step in comparative legal analysis. Dannemann states that while the 'presence of minimum

[20] Ishwara Bhat, *'Comparative Method of Legal Research Nature, Process, and Potentiality' Ideas and Methods of Legal Research* (Oxford University Press 2019).
[21] Nils Jansen, 'Comparative Law and Comparative Knowledge' in Mathias Reimann and Reinhard Zimmermann (eds), *The Oxford Handbook of Comparative Law* (Oxford University Press, 2006) 305..
[22] John Bell, 'Legal Research and the Distinctiveness of Comparative Law' in Mark Van Hoecke (ed) *Methodologies of Legal Research: Which Kind of Method for What Kind of Discipline?* (Bloomsbury Publishing Plc, 2011).

similarity avoids absurdity in comparison, prevalence of differences avoids monotony and repetition'.[23] Flanagan and Ahern provides guidance on how to select a jurisdiction for comparison by stating that most researchers make a choice based on their knowledge of languages and by comparing common law countries with other common law countries.[24] With this in mind, Australia was chosen as the comparative jurisdiction firstly from a practical point of view as it is an English speaking, common law jurisdiction but also because Australia has been a world leader in developing a regulatory system to tackle online harms, specifically including IBSA as a key issue of focus. Justification for choosing Australia as the key comparator is provided in detail in the following section. Curran argues that in order to conduct successful comparative analysis one should engage in the 'immersion' of culture.[25] In order to achieve some cultural immersion, the researcher conducted interviews within Australia so to gain first-hand experience of the culture but also to learn from the insights of stakeholders based in Australia so to assist in the implementation of a successful comparative aspect of the research. Legrand highlighted that 'being critical at all times' is essential for effective comparative analysis.[26] As a result the researcher did not accept the Australian approach as best practice from the outset but rather analysed the functioning of the system and the OESC in particular with an aim to identify areas not only of merit but also areas in need of improvement in order to bring a rounded perspective to the proposals for reform in Ireland.

Justification for the selection of Australia as the jurisdictional comparison

Three rationales informed the decision to select Australia as the key jurisdictional comparator in this thesis. These were:

1. The Australian OESC was used as an influential model by the LRC when making recommendations on how best to tackle online harassment and harmful communications.

[23] Gerhard Dannemann, 'Comparative Law: Study of Similarities or Differences?' in Mathias Reimann and Reinhard Zimmermann (eds), *The Oxford Handbook of Comparative Law* (Oxford University Press, 2006) 305..

[24] Brian Flanagan & Sinead Ahern, 'Judicial Decision-Making and Transnational Law: A Survey of Common Law Supreme Court Judges' (2011) 60(1) International & Comparative Law Quarterly 1-28.

[25] Vivian Curran, 'Cultural Immersion, Difference and Categories in US Comparative Law' (1998) 46(1), American Journal of Comparative Law 43, 46. Roger Cotterrell, 'Comparative Law and Legal Culture' in Mathias Reimann and Reinhard Zimmermann (eds), *The Oxford Handbook of Comparative Law* (Oxford University Press, 2006), 709, 711.

[26] Pierre Legrand, 'Comparative Legal Studies and the Matter of Authenticity', (2006) 1(2), Journal of Comparative Law 365.

2. Australia has been identified in the literature as a leading jurisdiction in the field of online regulation and the OESC has been commended for its success.
3. Australia was also selected for feasibility reasons, including language, legal structure, and the existence of a body of reports and evidence that could be used to investigate the research questions.

Rationale One

The initial rationale for selecting Australia as a key comparator was due to the LRC's high regard for the Australian approach to online safety. In the LRC report on Harmful Communications and Digital Safety, the LRC concluded that Ireland should follow the Australian approach to online safety by establishing a similar office tasked with similar functions to the OESC.

> The Commission has therefore concluded that Ireland should follow the approach taken in Australia and therefore recommends that an office be established on statutory basis with dual roles in promoting digital and online safety and overseeing an efficient and effective take down procedure in relation to harmful digital communications.[27]

In this report the LRC recommended the establishment of a Digital Safety Commissioner which would promote digital and online safety and oversee and regulate a system of 'take down' orders for harmful digital communications. This recommendation inspired the author to question whether such a body would effectively remedy victims of IBSA. In order to assess the potential effect of the Irish proposed approach at the time (the Digital Safety Commissioner), an examination of the initial influencing body, the OESC, was necessary.

Rationale Two

In addition to the LRC report, the Australian approach and the OESC have been recognised internationally as a novel response to the particular challenge of online harm. Powell, Scott, Flynn, and Henry identified the work of the OESC as 'important',[28] while Mee described the Australian approach as 'leading the fight against online abuse'.[29] Stephens also described the Australian approach as 'leading the way'.[30] Flynn and Henry

[27] Law Reform Commission, Harmful Communications and Digital Safety (LRC 116 — 2016) 3.66.
[28] Anastasia Powell, Adrian J. Scott, Asher Flynn, and Nicola Henry, 'Image-Based Sexual Abuse: An International Study of Victims and Perpetrators' (Summary Report February 2020).
[29] Paul Mee, 'Leading the Fight Against Online Abuse' (Perspective, n.d) < Leading The Fight Against Online Abuse (marshmclennan.com)> (accessed 19 December 2022).
[30] Hugh Stephens, 'Grappling with Online Safety Legislation: How to Hold the Platforms Accountable' (2022) The International Forum for Responsible Media Blog.

describe the Australian approach as having 'some of the most advanced legislative responses to IBSA globally'.[31] Furthermore, Yar and Drew identified the consideration of the Australian approach as an 'opportunity to explore the benefits and possible pitfalls of a proactive and concerted effort to tackle the challenges of reporting, reacting to, and preventing IBA'. [32]

The eSafety Commissioner Julie Inman Grant also identified that other jurisdictions are looking to the Australian approach as a model in the IBSA context.

> It's encouraging that the EU is looking at our experience, because if Europe were to follow a similar path to Australia it would help to close the net around those seeking to trade and profit from this terrible content.[33]

Within Ireland, Deputy Niamh Smyth of Fianna Fáil commended the Australian approach for 'leading the way globally in the protection of people online'.[34] Slane identifies the potential for Canada to adopt a similar approach to Australia arguing that 'a similar co-regulatory regime for complaints about online content removal' should be established.[35]

In spite of the praise the Australian approach and institutions had received, it is important to examine the approach in a cautious and open-minded manner. The author did not assume the Australian approach to be without limitation but sought to use a victim-centred approach to identify any lessons from the Australian experience that could be applied to better address the needs of victims of IBSA in Ireland.

Rationale Three

On a practical level, Australia is an English-speaking common-law jurisdiction, which are key factors that aid its comparability with Ireland. Furthermore, Australia was the first jurisdiction to establish a statutory body to tackle online safety issues. In March 2015, the Enhancing Online Safety for Children Act became law in Australia. At the time the author

[31] Asher Flynn and Nicola Henry, 'Image-Based Sexual Abuse: An Australian Reflection' (2019) Women and Criminal Justice.
[32] Majid Yar and Jacqueline Drew, 'Image-Based Abuse, Non-Consensual Pornography, Revenge Porn: A Study of Criminalization and Crime Prevention in Australia and England & Wales' (2019) 13 International Journal of Cyber Criminology.
[33] Melissa Coade quoting Julie Inman Grant in - Melissa Coade, 'European Union representatives look to Australian model for online safety' (The Mandarin, 23 February 2022).
[34] Deputy Niamh Smyth, Joint Committee on Tourism, Culture, Arts, Sport and Media debate - Wednesday, 21 Jul 2021.
[35] Andrea Slane, 'Search Engines and the Right to Be Forgotten: Squaring the Remedy with Canadian Values on Personal Information Flow' (2018) 55 Osgoode Hall Law Journal.

was refining the jurisdictional scope of their research question, the only other jurisdiction developing a comparable response to online safety issues was New Zealand. In July 2015, the New Zealand Parliament enacted the Harmful Digital Communications Act 2015 which provided that harmful digital communications complaints be made initially to an 'Approved Agency'.[36] However, this 'Approved Agency' was not appointed until May 2016.[37] While both jurisdictions enacted laws establishing an approach to tackle online issues in 2015, the Australian model had released a six-month report by December 2015 on the functioning of its approach[38] while the New Zealand model was still awaiting implementation. As the Australian approach was implemented and developed first, this led to a greater body of reports and evidence to be considered by the author. Overall, the selection of Australia as the jurisdictional comparator was justified due to the cumulation of three factors; the evidence base already established in the Australian context considered together with the leading nature of the Australian approach as identified by relevant literature in the field and the reference to the Australian approach by the LRC.

Justification for the non-adoption of a gender-specific approach

In recent times, significant research has been conducted regarding IBSA as a gendered, minority-focused[39] and feminist issue.[40] While some studies have found that, similar to other forms of intimate aggression, women are more commonly the targets of IBSA as compared to men,[41] others have found similar victimization rates among both men and

[36] Harmful Digital Communications Act 2015.
[37] NetSafe was appointed as the 'Approved Agency' for the purposes of the Harmful Digital Communications Act 2015 NetSafe, 'What is the HDCA?' < What is the HDCA? - Netsafe – Providing free online safety advice in New Zealand> accessed (21 December 2022).
[38] Office of the Children's eSafety Commissioner, eSafety Six Month Report (31 December 2015).
[39] Nicola Henry & Asher Flynn, 'Image-Based Sexual Abuse: Online Distribution Channels and Illicit Communities of Support' (2019) 25(16)Violence Against Women 1932; Asher Flynn & Nicola Henry, 'Image-Based Sexual Abuse: An Australian Reflection' (2021) 31(4)Women & Criminal Justice 313; Walter DeKeseredy & Martin Schwartz, 'Thinking Sociologically about Image-Based Sexual Abuse: The Contribution of Male Peer Support Theory' (2016) Sexualization, Media, & Society 1-8; Clare McGlynn, Erika Rackley & Ruth Houghton, 'Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse'(2017) 25 Feminist Legal Studies 25; Sophie Maddocks, 'From Non-consensual Pornography to Image-based Sexual Abuse: Charting the Course of a Problem with Many Names'(2018) 33 Australian Feminist Studies 345.
[40] Clare McGlynn & Erika Rackley, 'Image-Based Sexual Abuse' (2017) 37 Oxford Journal of Legal Studies 534; Clare McGlynn, Erika Rackley, & Ruth Houghton, 'Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse' (2017) 25 Feminist Legal Studies 256; Elizabeth Farries, 'Feminist Legal Geographies of Intimate-Image Sexual Abuse: Using Copyright Logic to Combat the Unauthorized Distribution of Celebrity Intimate Images in Cyberspaces' (2019) 51 EPA: Economy and Space 1145.
[41] Marsha Wood, Chistine Barter, Nicky Stanley, Nadia Aghtaie & Cath Larkins, 'Images Across Europe: The Sending and Receiving of Sexual Images and Associations with Interpersonal Violence in Young People's Relationships' (2015) 59 Children and Youth Services Review 149; Michelle Gonzalez, 'Power in Numbers' **(**Cyber Civil Rights Statistics on Revenge Porn, 3 January 2014) < https://cybercivilrights.org/revenge-porn-infographic/> accessed 14 January 2022; Office of the eSafety Commissioner, 'National Survey on Image-Based Abuse in Australia' *Report prepared for the Office of the*

women.[42] In spite of this, the majority of research conducted to date has found that IBSA is predominantly targeted at women and perpetrated by men.[43] Not only are women the predominant victims in cases of IBSA, but they have also been the object of 'victim-blaming'. Henry, Flynn, and Powell argue that 'traditional masculine values, victim-blaming attitudes, and a lack of understanding of gendered violence' have contributed to the lack of law enforcement intervention in response to reports by women regarding IBSA.[44] While research adopting a gender-specific approach is vital in identifying prevalence, nature, harms, and or perpetration of IBSA – and indeed reference is made to these studies when outlining the scale of IBSA in Australia and Ireland – this thesis relies on doctrinal analysis, comparative analysis, and interviews in order to address the research questions. This does not dispute the value that a gender-specific approach may have in a project addressing these questions, but it was determined that a gender-specific approach was not necessary for the purposes of this thesis.

Justification for adopting a victim-centred approach

A recurring finding in the literature is the failure of traditional approaches and existing laws to address the needs of victims of IBSA.[45] The development of a new system of redress in Australia was an acknowledgment of the need for alternative approaches to address the challenge of online harms. The research on IBSA further strengthens the case

---

eSafety Commissioner (Melbourne: RMIT University, 2017); Nicola Henry, Asher Flynn & Anastasia Powell, 'Policing Image-Based Sexual Abuse: Stakeholder Perspectives' (2018) 19(6) Police Practice and Research 565; Jessica Ringrose & Emma Renold, 'Slut-Shaming, Girl Power and 'Sexualisation': Thinking Through the Politics of the International SlutWalks with Teen Girls' (2012) 24(3) Gender and Education 333.

[42] Amanda Lenhart, Michaelle Ybarra & Myeshia Price-Feeney, *Online Harassment, Digital Abuse and Cyberstalking in America Report 11.21.16* (Data and Society Research Institute); Anastasia Powell & Nicola Henry, 'Technology-Facilitated Sexual Violence Victimization: Results from an Online Survey of Australian Adults'(2019) 17 Journal of Interpersonal Violence 34; Lauren Reed, Richard Tolman, & Monique Ward, 'Snooping and Sexting: Digital Media as a Context for Dating Aggression and Abuse Among College Students' (2016) 22(13) Violence Against Women 1556.

[43] Michelle Gonzalez, 'Power in Numbers' **(**Cyber Civil Rights Statistics on Revenge Porn, 3 January 2014) < https://cybercivilrights.org/revenge-porn-infographic/> accessed 14 January 2022; Office of the eSafety Commissioner, 'National Survey on image-based abuse in Australia' *Report prepared for the Office of the eSafety Commissioner* (Melbourne: RMIT University, 2017); Nicola Henry, Asher Flynn & Anastasia Powell, 'Policing Image-Based Sexual Abuse: Stakeholder Perspectives' (2018) 19(6) Police Practice and Research 565

[44] Nicola Henry, Asher Flynn & Anastasia Powell, 'Policing Image-Based Sexual Abuse: Stakeholder Perspectives' (2018) 19(6) Police Practice and Research 565.

[45]Nicola Henry, Asher Flynn and Anastasia Powell, 'Responding to 'revenge pornography': Prevalence, nature and impacts' Report to the Criminology Research Advisory Council Grant: CRG 08/15-16 (March 2019); Anastasia Powell & Nicola Henry, 'Policing technology-facilitated sexual violence against adult victims: police and service sector perspectives' (2018) 28 Policing and Society 301; Anastasia Powell, Nicola Henry, Adrian Scott & Asher Flynn, *Image-based sexual abuse: An international study of victims and perpetrators. Summary Repor*t (February 2020); D. Cook, 'Revenge pornography' (2015) 179 Criminal Law and Justice Weekly 152; Office of the eSafety Commissioner, *Image-Based Abuse Qualitative Research Summary* (October 2017).

that a different approach is necessary to adequately address the needs of victims in this context. As argued by McGlynn and others, a better understanding of 'the holistic and comprehensive nature of the harms of image-based sexual abuse … should help to shift law and policy debates towards more comprehensive and effective responses.'[46] This thesis adopts a victim-centred approach by quite explicitly centring the needs of victims of IBSA and making practical recommendations based on fulfilling those needs. To assist with the victim-centred approach, this thesis develops a framework illustrating the relationship between the needs of victims and various tools/mechanisms with the potential to respond to those needs and applying and refining that framework in different contexts. In order to develop a victim-centred policy response to IBSA, it is necessary to understand the particular harms of IBSA and to identify the needs of victims of IBSA. Once these harms and needs are clearly identified, this thesis considers what tools/mechanisms may best assist in the addressing of those needs.

Victim-centred approaches stem from theories of victimology.[47] Prominent early researchers in the field of victimology focused on the 'role that victims played in crime, which resulted in the concept that some victims contribute to, or precipitate, their victimisation'.[48] However, by the 1970's these ideas were regarded as 'victim-blaming'[49] and instead victimologists focused on the 'process of victimisation, including the treatment of victims in the criminal justice system'.[50] Fattah explained that the use of this knowledge is to 'prevent criminal victimisation, not to blame victims'.[51] Karem describes victimology as the study of 'the public's political, social, and economic reactions to the plight of victims'.[52] Consequently, within victimology there is a particular emphasis on

[46] Clare McGlynn, Kelly Johnston, Erika Rackley, Nicola Henry, Nicola Gavey, Anastasia Powell, and Asher Flynn, ''It's Torture for the Soul': The Harms of Image-Based Sexual Abuse' (2020) 30(4) Social and Legal Studies 541-562.

[47] Marianne Inéz Lien & Jørgen Lorentzen, *Men´s Experiences of Violence in Intimate Relationships* (Palgrave Macmillan 2019) 2. The field of victimology emerged in the 1940s after World War II with a purpose of gaining 'a better understanding of crime'. Michael O'Connell, 'Victimology: A Social science in Waiting?' (2008) 15 International Review of Victimology 91.

[48] Michael O'Connell, 'Victimology: A Social science in Waiting?' (2008) 15 International Review of Victimology 91; Hans Von Hentig, *The Criminal and His Victim* (Yale University Press 1948); Benjamin Mendelsohn, 'Une Nouvelle Branche de la Science Bio-Psycho-Sociale, la Victi-mologie' (1956) Etudes Internationales de Psycho-Sociologie Criminelle; Benjamin Mendelsohn, The Origin of the Doctrine of Victimology. In I. Drapkin and E. Viano (eds.), Victimology (Lexington Books 1974); Martin Wolfgang, 'Victim Precipitated Criminal Homicide' (1957) 48 Journal of Criminal Law and Criminology and Political Science; Willem Nagel, 'The Notion of Victimology in Criminology' (1963) 3 Excerpta Criminologica.

[49] Lorenne Clark and Debra Lewis, *Rape: The Price of Coercive Sexuality* (Women's Press 1977).

[50] Michael O'Connell, 'Victimology: A Social science in Waiting?' (2008) 15 International Review of Victimology 91.

[51] Ezzat Fattah, Understanding Criminal Victimisation (Prentice-Hall 1991).

[52] Andrew Karmen, *Crime victims: An introduction to victimology*, (9th edn, Cengage Learning 2015).

'victimisation'[53], 'repeat abuse'[54] and 'victim withdrawal from the criminal justice system'.[55]

Overall, victimology is research conducted with the aim of 'putting the victim at the centre'.[56]

> Victimology is not about the criminal justice system, nor is it about the helping system. Rather, it is about the victim; therefore, the victim must be the foci of the concepts, the theories and so on.[57]

This entails 'the application of knowledge to programmes and other initiatives to improve practical outcomes for victims'.[58] Relatedly, a victim-centred approach places emphasis on the experience of victims. In the context of this thesis, a victim-centred approach is adopted in order to explore how the needs of victims can best be met in the legislative response to IBSA.

There has been a 'growing emphasis on meeting the needs and rights of victims of crime in criminal justice policy and practice'.[59] For example, Barclay and Skarlicki identify the importance of considering victim perspectives and searching for 'outcomes that are victim-centred' and call for more research conducted from the 'perspective of people experiencing injustices'.[60] Hamber and Lundy's research identifies that 'addressing victims' needs should be at the center and drive approaches and processes for both transitional justice and historical institutional abuse'.[61]

Victim-centred approaches have particular value in the context of sexual offences. Notably, the United Nations High Commissioner for Refugees issued the first UN policy

---

[53] Marie Crandall, Avery Nathens, Mary Kernic, Victoria Holt and Frederick Rivara, 'Predicting Future Injury Among Women in Abusive Relationships' (2004) 56 The Journal of Trauma: Injury, Infection, and Critical Care.

[54] Lauren Bennett Cattaneo, Margaret Bell, Lisa Goodman and Mary Ann Dutton, 'Intimate Partner Violence Victims' Accuracy in Assessing their Risk of Re-Abuse' (2007) 22 Journal of Family Violence.

[55] Amanda Robinson and Dee Cook, 'Understanding Victim Retraction in Cases of Domestic Violence: Specialist Courts, Government Policy, and Victim-Centred Justice' (2006) 9 Contemporary Justice Review.

[56] Michael O'Connell, 'Victimology: A Social science in Waiting?' (2008) 15 International Review of Victimology 101.

[57] Ibid.

[58] Michael O'Connell, 'Victimology: A Social science in Waiting?' (2008) 15 International Review of Victimology 101.

[59] Marianne Inéz Lien & Jørgen Lorentzen, *Men´s Experiences of Violence in Intimate Relationships* (Palgrave Macmillan 2019)2.

[60] Laurice Barclay and Daniel Skarlicki, 'Shifting Perspectives: Helping Victims Recover From Organizational Justice Violations' (2008) 6 Research in Social Issues in Management 155-199; Debra Shapiro, 'The Death of Justice Theory is Likely if Theorists Neglect the "Wheels" Already Invented and the Voices of the Injustice victims (2011) 58 Journal of Vocational Behaviour 235-242.

[61] Brandon Hamber and Patricia Lundy, 'Lessons from Transitional Justice? Toward a New Framing of a Victim-Centered Approach in the Case of Historical Institutional Abuse' (2020) 15 Victims and Offenders 744.

of its kind in December 2020 endorsing a victim-centred approach in response to sexual misconduct.[62] It focuses on ensuring the safety, rights, well-being and expressed needs and choices of victims when responding to sexual misconduct. In the Irish context, the Irish Minister for Justice, Helen McEntee has stated that:

> We must work together to tackle and reduce the levels of these terrible crimes, and where an offence is committed, and where a wrong is done, we must ensure that all necessary supports are in place so that victims will feel safe and supported when they come forward (…) To do this, we must have in place a victim-centred approach. I want the victims of sexual crimes to know that they will be listened to, that they will be treated with respect and dignity, and that they will be supported throughout the process.[63]

In the context of sexual exploitation, Connors calls for the 'institutionalisation of a victim-centred approach' highlighting that giving 'visibility and a voice for victims' is a priority.[64] Connors further stated that there needs to be a core focus of 'providing victims with a voice that the world cannot ignore'.[65]

While the importance of adopting a victim-centred approach has been highlighted across various disciplines that consider vulnerable populations, its importance is particularly evident in the IBSA context. In adopting a victim-centred approach to the challenge of IBSA, this thesis draws from the work of Australian-based scholars, Henry, Powell, and Flynn, who have been leaders in advocating for the importance of representing victims in academic scholarship with the hope of encouraging legal and policy reform. Henry, Powell, and Flynn seek:

> recognition of the harms of image-based abuse on behalf of victims, advocate for legal and policy reform, and challenge community attitudes that blame the victims and excuse the perpetrators of image-based abuse.[66]

This thesis draws from their work and the work of other prominent IBSA scholars – including McGlynn, Rackley, Johnston, and Gavey – by adopting as a key principle that

---

[62] The UN Refugee Agency, Policy on a Victim-Centred Approach in UNHCR's response to Sexual Misconduct (UNHCR/HCP/2020/04); The UN Refugee Agency, 'A Victim-Centred Approach' <https://www.unhcr.org/victim-care.html> accessed 10 May 2023; United Nations , 'Victims' Rights First' <https://www.un.org/en/victims-rights-first> accessed 10 May 2023

[63] Department of Justice, 'Tackling sexual violence and building a victims centred approach a priority - Minister McEntee' (Press Release, 6 August 2020) < gov.ie - Tackling sexual violence and building a victims centred approach a priority - Minister McEntee (www.gov.ie)> accessed 10 May 2023.

[64] Jane Connors, A Victims' Rights Approach to the Prevention of, and Response to, Sexual Exploitation and Abuse by United Nations Personnel' (2019) 25 Australian Journal of Human Rights 503.

[65] ibid.

[66] Nicola Henry, Anastasia Powell and Asher Flynn, 'Not Just 'Revenge Pornography': Australians Experience of Image-Based Abuse' (Summary Report, 2017).

the experiences of victims must provide the foundation for the response to IBSA. In order to evaluate the effectiveness of a response to IBSA, this thesis asks what the needs of IBSA victims are and how can those needs be best met. This thesis seeks to discern this information from desk-based research drawing on academic literature and reports and in particular drawing on lessons from the Australian context. These findings are further informed by conducting interviews with key Australian-based stakeholders with expertise on online harm and IBSA. By investigating these questions, it is hoped that policy makers will better understand the nature of the harms of IBSA and 'help to shift law and policy debates towards more comprehensive and effective responses'.[67]

As put by Rackley, McGlynn, Johnston, Henry, Gavey, Flynn, and Powell:

> Now is not the time for tinkering around the edges of current law and support. It is time to listen to victim-survivors of image-based sexual abuse, taking their experiences and perspectives as the foundation from which to build a co-ordinated strategy. It is time for political leadership and targeted resources. It is time for fundamental change.[68]

The work of Henry, Flynn, and Powell has been leading in identifying the needs and experiences of victims 'pursuing legal or non-legal responses' against IBSA.[69] In order to gain insight into victim experiences, Henry, Flynn, and Powell have engaged in interviews with stakeholders in relation to policing and IBSA.[70] Interviewing stakeholders provides insight from those who are often at 'the frontline of responding to victims'[71] including 'legal and policy experts, domestic and sexual violence advocates, industry representatives, police, and academics'.[72] Understanding the perspectives of stakeholders is important as it allows for further exploration into the 'complexities of the

[67] Clare McGlynn, Kelly Johnston, Erika Rackley, Nicola Henry, Nicola Gavey, Anastasia Powell, and Asher Flynn, ''It's Torture for the Soul': The Harms of Image-Based Sexual Abuse' (2020) 30(4) Social and Legal Studies 541-562.
[68] Erika Rackley, Clare McGlynn, Kelly Johnson, Nicola Henry, Nicola Gavey, Asher Flynn and Anastasia Powell, 'Seeking Justice and Redress for Victim Survivors of Image Based Sexual Abuse' (2021) 29 Feminist Legal Studies 319.
[69] Nicola Henry, Asher Flynn & Anastasia Powell, 'Policing Image-Based Sexual Abuse: Stakeholder Perspectives' (2018) 19 Police Practice and Research 566; Asher Flynn and Nicola Henry, 'Image-Based Sexual Abuse: An Australian Reflection' (2019) Women and Criminal Justice; Nicola Henry, Asher Flynn and Anastasia Powell, 'Image-based sexual abuse: Victims and perpetrators' (2019) 572 Trends & Issues in Crime and Criminal Justice; Nicola Henry and Asher Flynn, 'Image-Based Sexual Abuse: Online Distribution Channels and Illicit Communities of Support' (2019) 25 Violence against Women 1950.
[70] Nicola Henry, Asher Flynn & Anastasia Powell, 'Policing Image-Based Sexual Abuse: Stakeholder Perspectives' (2018) 19 Police Practice and Research 566.
[71] Nicola Henry, Asher Flynn & Anastasia Powell, 'Policing Image-Based Sexual Abuse: Stakeholder Perspectives' (2018) 19 Police Practice and Research 566.
[72] ibid.

phenomenon'[73] and adult victimisation in 'technology-facilitated sexual violence'.[74] By interviewing individuals tasked with responding to victims of technology facilitated sexual violence, Powell and Henry have made progress in understanding 'the nature of the harms experienced' by victims and in determining 'some of the challenges in pursuing legal and non-legal responses'. [75] The prior work discussed above illustrates the role of empirical research in discerning victim-centred understandings and accordingly supports the use of interviews in this thesis to further inform the victim-centred approach adopted.

A key motivation for adopting a victim-centred approach in this area is that the traditional approaches appeared to be lacking from the perspective of victims. Some of the issues identified with the response to IBSA in the Australian context in 2019 included 'underreporting, inconsistent laws, a lack of resources, evidentiary limitations, jurisdictional restrictions, and victim-blaming attitudes that minimise and trivialise impacts and prevent victims from reporting to authorities'.[76]

McGlynn, Johnston, Rackley, Henry, Gavey, Powell, and Flynn highlight the importance of considering victim perspectives as it allows for victim empowerment and allows victims to 'better articulate and comprehend their experiences'.[77] As simply stated by the North Yorkshire Police, Fire and Crime Commissioner Julia Mulligan, a key aim for considering victims perspectives is to 'understand the challenges in supporting victims of revenge porn'.[78]

Hamber and Lundy argue that 'the starting point in any victim-centered process should be to determine victims' needs'.[79] In line with this reasoning, this thesis sets out to develop a framework informed by identifying victim needs and to apply this framework to evaluate the effectiveness of legislative measures designed to address IBSA. Due to

---

[73] Nicola Henry, Asher Flynn & Anastasia Powell, 'Policing Image-Based Sexual Abuse: Stakeholder Perspectives' (2018) 19 Police Practice and Research 575.
[74] Anastasia Powell and Nicola Henry, 'Policing Technology-Facilitated Sexual Violence Against Adult Victims: Police and Service Sector Perspectives' (2018)28 Policing and Society.
[75] ibid.
[76] Nicola Henry, Asher Flynn and Anastasia Powell, 'Image-based sexual abuse: Victims and perpetrators' (2019) 572 Trends & Issues in Crime and Criminal Justice 2.
[77]Clare McGlynn, Kelly Johnston, Erika Rackley, Nicola Henry, Nicola Gavey, Anastasia Powell, and Asher Flynn, ''It's Torture for the Soul': The Harms of Image-Based Sexual Abuse' (2020) 30(4) Social and Legal Studies 541-562.
[78] Julia Mulligan, North Yorkshire Police, Fire and Crime Commissioner, 'Commissioner welcomes Law Commission proposals to give anonymity to revenge porn victims' < Commissioner welcomes Law Commission proposals to give anonymity to revenge porn victims - Police, Fire and Crime Commissioner North Yorkshire (northyorkshire-pfcc.gov.uk) > accessed 21 May 2023.
[79] Brandon Hamber and Patricia Lundy, 'Lessons from Transitional Justice? Toward a New Framing of a Victim-Centered Approach in the Case of Historical Institutional Abuse' (2020) 15 Victims and Offenders 758.

the leading role Australia has taken in developing an innovative approach to online harms including IBSA, this thesis uses insights gained from the Australian experience to develop a framework to evaluate the effectiveness of legislative measures designed to address IBSA. As shown in Chapter 2, the author identifies key needs and potential tools/mechanisms of redress which are then used to assess whether the Irish response to IBSA addresses victim needs. The framework developed in Chapter 2 will be applied and considered throughout this thesis and represented in table form.

Structure of thesis

This thesis is divided into six chapters. Chapter 1 introduces the key concepts, technologies, terms, and rights which will be referenced throughout this thesis in order to provide a foundation for later discussions. Chapter 2 introduces the Australian legislative response to IBSA and sets out the victim-centred framework that will be applied throughout the thesis. As part of this, Chapter 2 examines the prevalence of IBSA within Australia and the development of laws criminalising IBSA. This chapter identifies issues with the criminal law in remedying victims of IBSA. Following this, Chapter 2 conducts a desk-based assessment of the Australian regulatory system addressing online safety and analyses the incremental development of that system. Particular attention is paid to the structure and powers of the OESC and the body's accounting of its activities through its published annual reports. Drawing from this analysis of Australian policy, law, and academic literature, the key needs of IBSA victims are determined and tools/mechanisms with potential to address those needs, at least in part, are identified. This provides the basis of a framework upon which to assess Irish legislative and policy decisions in later chapters. Chapter 3 advances this analysis by delving deeper into identifying the merits and limitations of the functioning of the OESC in practice by conducting interviews with key stakeholders in the area of online safety and regulation. The victim-centred framework developed in Chapter 2 is reconsidered in Chapter 3 in light of the findings made through conducting the interviews. Chapter 4 assesses the Irish situation by providing contextual background to policy and legal developments in the area of IBSA and mapping progress in the area over time up to the point of the implementation of targeted criminal legislation against IBSA. These developments are assessed to establish whether the Irish regulatory approach to IBSA up to the introduction of the Online Safety and Media Regulation Bill (now enacted as the Online Safety and Media Regulation Act) adequately addressed victim needs. Chapter 5 analyses Irish provision for a statutory online safety regulator. Drawing on lessons learned from the examination of the

Australian experience, Chapter 5 assesses the nascent system of regulation and makes recommendations for its future development. These recommendations are informed by the victim-centred framework as established and refined in the previous chapters. Finally, Chapter 6 summarises the key findings from the thesis and offers recommendations from a victim-centred perspective.

(5) Contribution

In 2017, McGlynn and Rackley highlighted Ireland's opportunity to introduce effective legislation to criminalise IBSA and become a leading jurisdiction in tackling this issue.[80] In spite of this, Ireland has been relatively laggard in this area, only criminalising IBSA in 2020. While the LRC identified a need for a statutory body with powers related to IBSA back in 2016, there was a clear need for an in-depth study of how the Australian system – on which the LRC modelled its recommendations – was operating in practice. This project addresses this need and uses the knowledge gained to provide recommendations appropriate to the Irish context. As the Irish Government only recently established an OSC – with similarities but notable differences from the OESC model – an in-depth analysis of the OESC is crucial.

There is a dearth of research considering the perspectives of stakeholders on the effectiveness of the OESC. While many submissions have been made by Australian stakeholders to the Australian Government on how to conduct legislative reform, there is a lack of data gathered on specific aspects of the removal processes in the context of IBSA. In 2020, Minister McEntee highlighted the importance of the adoption of a 'victim-centred approach' to sex crimes in Ireland.[81] Minister McEntee highlighted IBSA in this context and called for the prioritisation of victims and their needs. This thesis adopts a victim-centred approach in order to develop policy recommendations that would support Minister McEntee's call. Crucially, the framework developed in this thesis can be used to assess current and future legislation and policy through the lens of victim needs. This research has a global impact. Ireland and Australia benefit directly from this research as the potential impact of the OSC and the actual impact of the OESC are explored. Several

[80] Clare McGlynn & Erika Rackley, 'More than 'Revenge Porn': Image-Based Sexual Abuse and the Reform of Irish Law' (2017) 14 Irish Probation Journal 38.

[81] Shauna Bowers and Vivienne Clarke, 'McEntee wants to see 'victim-centred approach' to sex crimes: Action plan will be before Government within 10 weeks, says Minister for Justice' *The Irish Times* (Dublin, 7 August 2020).

of the lessons learned have applicability outside of the Australian and Irish contexts and thus this research also has the potential to inform reform efforts in other jurisdictions.

Chapter 1: Understanding the context and development of image-based sexual abuse

1.1 Introduction

The proliferation of sexually explicit material shared online without consent is a growing concern in internet law. It has been the subject of much debate that has led to law reform in many jurisdictions. This chapter examines the concept and development of the act of image-based sexual abuse (IBSA)[1] and its link to technological change and the internet.

This chapter begins by defining the terms 'internet' and 'cyberspace' and discusses the evolution of the internet from 'web 1.0' to 'web 2.0' and the respective challenges posed by these developments. Since the internet is now such a fundamental factor in the creation and distribution of IBSA, its capabilities and parameters must be properly outlined. This linking of technology and the internet to the proliferation of IBSA is crucial as the increase in technical capabilities has led to a parallel increase in the ease with which perpetrators can carry out IBSA. Specific legal issues and enforcement challenges that tend to arise online are identified and considered in the context of IBSA.

The act of IBSA and its variations are more formally defined. 'Image Based Sexual Abuse' is a key term in this thesis and therefore is addressed in detail, with the scope of acts of IBSA being examined through consideration of a number of examples. Although IBSA is not a novel act, it has increased in prominence in recent times since it is greatly facilitated by technology. In section 1.3.4 below, the potential effects of IBSA on victims are explored. This includes discussion of a selection of victims' stories. These stories help inform the victim-centred perspective of this thesis and illustrate a number of important facts about the nature of IBSA and the harm it can cause. Shifting attitudes towards IBSA are also discussed.

This chapter also seeks to analyse the various platforms which facilitate IBSA. Technologies including the internet and social media have all impacted IBSA, from the way in which it is carried out to the harm that results. Particular focus is given to social

[1] The acronym 'IBSA' will be used throughout this thesis.

media platforms such as Facebook, Snapchat, and Instagram since they can facilitate the hosting and wide-scale distribution of IBSA material and are therefore favoured by many perpetrators. Additionally, the development of mobile phones and the resulting proliferation of social media applications associated with them has led to various practices such as 'sexting' and 'selfies' which may produce material or images that later may be used for the purposes of IBSA, so these concepts are also discussed.

Finally, this chapter provides an overview of how the regulation of the internet has developed over time. This section considers the legal safe harbours that were developed to protect online intermediaries from liability for the actions of users of their services and the more recent moves in favour of increased intermediary responsibility.

The discussion of the terms and concepts described above provides an overview of how IBSA is conducted, how technology and social media play a crucial role in the perpetration of IBSA, and the impacts of IBSA on victims. An in-depth understanding of the importance of the internet, technology, and social media is essential as a key aspect of this thesis is the discussion of efficient enforcement responses to assist in the removal of intimate images from social media platforms and the internet. Understanding these concepts also provides greater insight into the specific needs of IBSA victims and provides important context that assists the assessment of which tools and mechanisms have the potential to respond effectively to the needs of victims.

1.2 Challenges of regulating harmful activities on the internet

1.2.1 Defining the 'internet' and 'cyberspace'

One of the main functions of the internet is its role as a medium of communication whereby everyone who is on the network can communicate 'instantaneously and simultaneously'.[2] This function has greatly increased our capacity to enjoy freedom of expression. The internet has made it possible for people to interact spontaneously, correspond easily, express themselves freely, and to have a voice concerning a plethora of issues. It allows individuals to establish contacts with broad groups of people worldwide and foster closer ties with family, friends and other 'real world' contacts.[3] The interconnected nature of the internet is attributed mainly to the 'World Wide Web' which connects us from one web page to another via hyperlinks. It has facilitated a new form of

[2] David Post, 'Governing Cyberspace: The Law' (2008) 24 Santa Clara Computer and High Technology Law Review 883.
[3] Law Reform Commission, Harmful Communications and Digital Safety (LRC 116 — 2016) 1.01.

online and digital consumer society. Unlike during times before the advent of the internet when we could only visit shops in our own town or city or else be forced to travel, the internet allows us to see information offered on billions of web pages by millions of people and companies from all over the world.[4] We can move from a page in Paris to a page in New York merely by following a link.[5] This automatic connection that allows us to experience any part of the globe and engage with many communities is another notable function of the internet. David Kaye, the United Nations special rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, accurately highlighted these two functions stating that the internet 'has profound value for freedom of opinion and expression, as it magnifies the voice and multiplies the information within reach of everyone who has access to it so much so that it has become, within a relatively brief period the central global forum'.[6] However, these functions cannot be enjoyed by everyone, as research points out that there is still a 'digital divide,' a gap between those who have and do not have access to computers and the internet and between those who have and do not have skills in using computers and the internet.[7]

While the internet is well understood and utilised, it has a dark aspect that is important to highlight as it is part of its make-up and operation. This aspect is evident in two forms – the dark side and the darknet. Research suggests that people often confuse the dark side of the internet with the darknet and explain the darknet by describing the dark side of the internet.[8] Firstly, the internet has a dark side whereby it is used for nefarious or criminal purposes. Often those engaged in such activities use the same search engines, social media platforms, and websites as those engaged in positive or neutral activities. These acts include crimes that occur in the offline as well as the online world, such as stalking, harassing and defaming, and also acts that originated on the internet such

[4] Mark Lemley, 'Place and Cyberspace' (2003) 91 California Law Review 521.
[5] ibid.
[6] UN Human Rights Council, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (2015) A/HRC/29/32 [11].
[7] Martin Hilbert, 'The Bad News is that the Digital Access Divide is Here to Stay: Domestically Installed Bandwidths Among 172 Countries for 1986–2014' (2016) Telecommunications Policy; Jacob Vigdor, Helen Ladd & Erika Martinez, 'Scaling the Digital Divide: Home Computer Technology and Student Achievement' (2014) 52 Economic Inquiry 1103.
[8] Paul Farrell, 'Inside the Darknet: Where Australians Buy and Sell Illegal Goods' (The Guardian, 4 July 2017) <https://www.theguardian.com/technology/2017/jul/04/inside-the-darknet-where-australians-buy-and-sell-illegal-goods> accessed 16 February 2022; Cara McGoogan, 'Dark Web Browser Tor is Overwhelmingly Used for Crime, Says Study' *The Telegraph* (London, 2 February 2016); Adam Samson, 'Dark Net May Pose 'Disruptive Risk' to Internet Sector—Goldman' *Financial Times* (London, 13 July 2017).

as catfishing or phishing.[9] Secondly, there is an area of the internet that is not found by standard search engines, which is known as the 'Darknet' or 'Dark Web'. It is a subsection of the 'Deep Web' and exists as a 'private network' in which 'peers' or 'friends' connect by way of nonstandard protocols and ports.[10] Unlike some other peer-to-peer networks, sharing on the Darknet is anonymous, and internet protocol (IP) addresses are not shared publicly, so that users do not have to fear the risk of exposure.[11]

Although it was not originally launched for any malicious purpose, the Darknet is known to facilitate crime. It facilitates the distribution of indecent images of children, cyber-security threats, the trading of weapons,[12] exotic animals,[13] credit card and personal information, [14] and other illegal goods. [15] Research by Dolliver, Owen, and Savage suggests the trading of illegal drugs is the most prevalent activity on the Darknet.[16] In January 2016, total drug revenues on the Darknet, excluding prescription drugs, were estimated to be between $12 million and $21.1 million.[17] Various technological characteristics of the network such as anonymity, privacy, and the use of cryptocurrencies, have enabled the growth of Darknet markets.[18] It has facilitated a tendency among some online and digital users to engage in communication that causes significant harm to others,[19] and that they would not have otherwise engaged in in real space or on the conventional internet.

---

[9] Phishing is a type of internet scam in which the perpetrator sends out false e-mail that appears to come from a legitimate source, in an effort to gather useful data such as credit card information, PINs, and passwords.

[10] Elisa D'Amico & Luke Steinberger, 'Fighting for Online Privacy with Digital Weaponry: Combating Revenge Pornography' (2015) 26 NYSBA Entertainment, Arts and Sports Law Journal 24.

[11] ibid.

[12] BBC, 'Dark Net Guns Shipped in Old Printers' (BBC News, 20 July 2017) <https://www.bbc.com/news/technology-40668749 > accessed 16 February 2022.

[13] Michael Chertoff & Tobby Simon, 'The Impact of the Dark Web on Internet Governance and Cyber Security' Global Commission on Internet Governance (Paper Series No. 6 — February 2015).

[14] Eric Holm, 'The Darknet: A New Passageway to Identity Theft' (2017) 6(1) International Journal of Information Security and Cybercrime 41–50.

[15] Michael Chertoff & Tobby Simon, 'The Impact of the Dark Web on Internet Governance and Cyber Security' Global Commission on Internet Governance (Paper Series No. 6 — February 2015).

[16] Diana Dolliver, 'Evaluating Drug Trafficking on the Tor Network: Silk Road 2, the Sequel' (2015) 26(11) International Journal of Drug Policy 26 1113–1123; Gareth Owen & Nicolas Savage, 'Empirical Analysis of Tor Hidden Services' (2016) 10(3) IET Information Security 113–118.

[17] Kristy Kruithof, Judith Aldridge, David Décary Hétu, Megan Sim, Elma Dujso, & Stijn Hoorens, *Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands* (Santa Monica, Calif.: RAND Corporation, RR-1607-WODC, 2016).

[18] Mihnea Mirea, Victoria Wang, & Jeyong Jung, 'The not so dark side of the darknet: a qualitative study' (2019) 32(2) Security Journal 102.

[19] Law Reform Commission, Harmful Communications and Digital Safety (LRC 116, 2016) 1.01.

However, the Darknet is used not only by criminals. While the Darknet is certainly used by some individuals to carry out illicit activities,[20] the Darknet may be used to carry out legitimate actions. They include activities of activism, journalism, and whistleblowing. Individuals may use the anonymity the Darknet provides for social and political purposes by openly sharing their social and political beliefs without fear of retribution.[21] This sharing is especially necessary in countries with strong State censorship and surveillance against political activists, freedom fighters, and journalists.[22] Journalists, activists, and whistle-blowers in these countries may use the Darknet to communicate with the outside world, encourage social change, and political reform, without disclosing their identities.[23]

The internet has become enmeshed in our daily lives and has become a crucial means of carrying out everyday tasks. Networked interactions are embedded in real life.[24] This notion that the internet and real life are connected was discussed in the 1990s through the term 'cyberspace'.[25] Cyberspace was described as a 'virtual world' built like a layer on top of the internet and connected via a computer.[26] Today, the term 'cyberspace' is dated and the term 'internet' encompasses the notion that life online is connected to life offline, and vice versa.[27] The internet enables users to encounter, interact and communicate in a similar manner as in the real world.[28] Many aspects of life can occur in cyberspace as they do in the 'real world' – paying a bill, shopping, chatting to a friend, meeting a friend or sharing a photo. It involves activities that cause real-world effects.[29] As Cohen has noted, 'the digital and the physical world are enmeshed. We cannot "log out"'.[30]

1.2.2 Challenges in web 1.0

[20] Mihnea Mirea, Victoria Wang, & Jeyong Jung, 'The not so dark side of the darknet: a qualitative study' (2019) 32(2) Security Journal 102.
[21] Daniel Moore & Thomas Rid, 'Cryptopolitik and the Darknet' (2016) 58 (1) Survival Global Politics and Strategy 7.
[22] Eric Jardine, 'The Dark Web Dilemma: Tor, Anonymity and Online Policing' Global Commission on Internet Governance. (Paper Series No. 21 — September 2015).
[23] Michael Chertoff & Tobby Simon, 'The Impact of the Dark Web on Internet Governance and Cyber Security' Global Commission on Internet Governance (Paper Series No. 6 — February 2015).
[24] Danielle Citron, *Hate Crimes in Cyberspace* (1st edn, Harvard University Press 2016) 20.
[25] Jack L. Goldsmith, 'Against Cyberanarchy' (1998) 65 University of Chicago Law Review 1199.
[26] Lawrence Lessig, *Code Version 2.0* (2nd edn, Basic Books 2006) 9.
[27] Danielle Citron, *Hate Crimes in Cyberspace* (1st edn, Harvard University Press 2016) 20.
[28] Lawrence Lessig, *Code Version 2.0* (2nd edn, Basic Books 2006) 83.
[29] Jack L. Goldsmith, 'Against Cyberanarchy' (1998) 65 University of Chicago Law Review 1199.
[30] Julie Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (New Haven, CT: Yale University Press 2012).

Although the internet has a long history, dating back to 1969, much of its early years were hidden away in universities and research labs.[31] The internet started to become more widely accessible in the early 1990s when Berners-Lee and Cailliau's hypertext-based world wide web application[32] was revealed to the public. This development, which many observers call 'web 1.0,' gave people their first experience of a computer communications tool[33] in the form of internet forums. An internet forum or message board is an online exchange system that allows a person to leave a message which may be read by other users at a later date. Other forms of communication experienced on web 1.0 included personal websites. These websites were different from forums as they were not interactive but allowed people to write about their views for others to read. However, viewers of the content could not engage with the material. These initial functions of the internet provided many benefits. They included the ability to make the world seem like a smaller place, allowed people to communicate with large audiences, and offered new ways to conduct business.[34] However, the merits also brought limitations and challenges. Research found that web 1.0 internet forums positively reinforced the actions of child abusers, allowing them to connect.[35] It also facilitated the trading of indecent images of children.[36] A study conducted by the US National Centre for Missing and Exploited Children tracked indecent images of children in peer-to-peer networks in 2001. It showed that indecent images of children available within these systems had increased by 400% over two years.[37] Internet forums and personal websites could also be used for criminal activities such as money laundering and support for terrorists.[38]

1.2.3 Challenges in web 2.0

A dynamic, interactive and socially connected web experience known as 'web 2.0' has since replaced the static web pages and internet forums. Tim O'Reilly, who helped coin

---

[31] National Research Council, Funding a Revolution: Government Support for Computing Research (National Academy Press 1999) 175.
[32] Tim Berners-Lee, Robert Cailliau, Jean-François Groff, Bernd Pollermann 'World Wide Web: The Information Universe' (1992) 2 Electronic Netwroking 52.
[33] Andrew Murray, *Information Technology Law and Society* (3rd edn, New York: Oxford University Press 2016).
[34] Andrew Murray, *Information Technology Law and Society* (3rd edn, New York: Oxford University Press 2016).
[35] Marie Eneman, 'The New Face of Child Pornography' in Mathias Klang and Andrew Murrary (eds) *Human Rights in the Digital Age* (Routledge-Cavendish 2005).
[36] ibid.
[37] Linda Koontz, 'File Sharing Programs, Users of Peer-to-Peer Networks Can Readily Access Child Pornography' (United States General Accounting Office Report GAO-03-1115T, 2003).
[38] Andrew Murray, *Information Technology Law and Society* (3rd edn, New York: Oxford University Press 2016).

the term 'web 2.0', provides a definition by stating: 'web 1.0 was about connecting computers and making technology more efficient for computers. Web 2.0 is about connecting people and making technology more efficient for people'.[39] Unlike the brochure-like static web pages from web 1.0, web pages now carry multiple functions allowing the viewer to engage through drop-down bars, search tools, direct messaging and shopping carts. Not only can users publish and view material; they can also instantly reply, upload images, tag friends, invite friends, share videos, etc. Interactivity is at the heart of web 2.0.[40] Web 2.0 has revolutionised society and changed the way people live. Simple tasks such as paying a bill, shopping, booking a hotel or banking have all been revolutionised. Due to the development of web 2.0, we now have multiple options as to how we live, learn and communicate. Web 2.0 continues to create new ways for large groups of people to collaborate and exchange information while reducing the importance of the computer itself as an information-delivery platform.[41] As long as the applications and the data reside online, a variety of devices, such as smartphones, music players or computers, can function as information terminals.[42]

Since web 2.0 has been characterised as the 'read and write'[43] web, user-generated content plays a vital role in its characterisation. User-generated content is material that is produced by the audience or users of a medium. It is an essential means by which people can express themselves and communicate with others online.[44] It is produced in the moment of being social, as well as the object around which sociality occurs.[45] User-generated content takes on many different forms, such as Twitter tweets, Facebook status updates and videos on YouTube, as well as consumer-produced product reviews and advertisements.[46]

---

[39] Tim O'Reilly, 'What Is Web 2.0? Design Patterns and Business Models for the Next Generation of Software' (2003) <https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html> accessed 20 February 2022.
[40] Andrew Murray, *Information Technology Law and Society* (3rd edn, New York: Oxford University Press 2016).
[41] Beverly Crane, *Using Web 2.0 and Social Networking Tools in the K-12 Classroom* (American Library Association 2012).
[42] Beverly Crane, *Using Web 2.0 and Social Networking Tools in the K-12 Classroom* (American Library Association 2012).
[43] Danah M. Boyd & Nicole B. Ellison, 'Social Network Sites: Definition, History, and Scholarship' (2008) 13
Journal of Computer-Mediated Communication 210.
[44] ibid.
[45] Andrew Smith, Eileen Fischer, & Chen Yongjian, 'How Does Brand-related User-generated Content Differ across YouTube, Facebook, and Twitter?' (2012) 26 Journal of Interactive Marketing 102.
[46] Albert M. Muñiz Jr., Hope Jensen, & SchauVigilante, 'Marketing and Consumer-Created Communications' (2007) 36(3) Journal of Advertising 35; Vasant Dhar & Elaine A. Chang, 'Does Chatter

Web 2.0 provides a critical social aspect as it is not only used to gather information or carry out a task but also to socialise, meet new people, and build relationships. The key providers of this interconnected internet experience are social media platforms such as Facebook, YouTube, Twitter, and Instagram. Social media provides a link between people and communities and allows people to interact in many ways. These interactions include direct messaging, video calls, posting comments, sharing media such as videos or photos, engaging in surveys, and playing virtual games. Web 2.0 has facilitated the development of dating apps and websites, which are online or mobile platforms where people can meet potential romantic or sexual partners.[47] One study found that approximately 15% of all US adults have reported using online dating apps or websites.[48] It is yet another example of the social element to web 2.0.

Web 2.0 is a 'double-edged sword' that provides many opportunities for individuals and organisations to develop and prosper but at the same time has brought new opportunities to commit crimes.[49] Web 2.0 not only facilitates the perpetration of traditional crimes in the online environment, such as sharing indecent images of children, stalking, bullying and harassment; it has also resulted in new harms such as creating fake profiles and catfishing. Catfishing has been described as 'the current internet trend of creating and portraying complex fictional identities through online profiles'.[50] Catfishing can also involve financial exploitation. For example, scammers might commit identity fraud or pretend to maintain an intimate and trusting relationship with another individual in the hope of receiving money from them.[51] A study using a sample of users of heterosexual dating websites found that around 80% of respondents included content in their profile that was at variance with at least one of their observable characteristics.[52]

Matter? The Impact of User-Generated Content on Music Sales' (2009) 23(4) Journal of Interactive Marketing 300.

[47] Carolyn Lauckner, Natalia Truszczynski, Danielle Lambert, Varsha Kottamasu, Saher Meherally, Anne Marie Schipani-McLaughlin, Erica Taylor & Nathan Hansen, 'Catfishing, Cyberbullying, and Coercion: An Exploration of the Risks Associated with Dating App Use Among Rural Sexual Minority Males' (2019) 23(3) Journal of Gay & Lesbian Mental Health 289.

[48] Aron Smith, *15% of American adults have used online dating sites or mobile dating apps* (Washington, DC: Pew Research Center 202.419.4372 — February 2016).

[49] Peter Gottschalk, *Policing Cyber Crime* (1st edn, Bookboon 2010).

[50] Meaghan P. Nolan, 'Learning to circumvent the limitations of the written-self: The rhetorical benefits of poetic fragmentation and internet 'catfishing'' (2015) 1(1) Persona Studies 53.

[51] Carolyn Lauckner, Natalia Truszczynski, Danielle Lambert, Varsha Kottamasu, Saher Meherally, Anne Marie Schipani-McLaughlin, Erica Taylor & Nathan Hansen, 'Catfishing, cyberbullying, and coercion: An exploration of the risks associated with dating app use among rural sexual minority males' (2019) 23(3) Journal of Gay & Lesbian Mental Health 289.

[52] Catalina L. Toma, Jeffery T. Hancock, & Nicole B. Ellison, 'Separating fact from fiction: An examination of deceptive self-presentation in online dating profiles' (2008) 34(8) Personality and Social Psychology Bulletin 1023.

1.2.4 Specific legal issues raised in the online context

A kind of 'euphoria' greeted the internet.[53] It was viewed in a positive light, and people felt liberated and free upon its arrival.[54] The internet revolutionised self-expression and enhanced freedom, giving unprecedented new ways of communicating privately and publicly to a worldwide audience. However, with the internet no longer in its infancy, challenges have also arisen.[55] Difficulties with the enforcement of laws online – in the face of issues like anonymising capabilities and jurisdictional barriers – have created a sense of impunity in some contexts.

Application of the law to the internet

The internet is a 'complex, anarchic and multi-national environment where old concepts of regulation, reliant as they are upon tangibility in time and space, may not be easily applicable or enforceable'.[56] Regulating the internet remains a challenge. Due to the continual development of new technologies that weave themselves into our lives, legal challenges are continually surfacing. As a result, society often has to apply 'old law' that is generally unsatisfactory as it 'relies on assumptions that are no longer true'.[57] The application of existing law to the internet is a challenge and causes many problems in all disciplines of law. Problems with regulating the internet have occurred due to existing laws being hard to adapt, or indeed inadaptable in some circumstances. The refashioning of existing, familiar principles to deal with new challenges has proven ineffective in many cases when dealing with the internet.[58] The attempted shoehorning of these laws has led to unsuccessful cases, leaving victims of online crimes without a remedy, including in the IBSA context.[59]

There is now a huge array of laws designed specifically to address the challenges of the internet age. The EU has a significant agenda on these matters and has taken a leading role in internet regulation, perhaps most famously through its approach to data protection

[53] Daniel Solove, *The Future of Reputation: Gossip, Rumor and Privacy on the Internet* (Yale University Press 2007) 4.
[54] Lawrence. Lessig, *The Future of Ideas: The fate of the Commons in a Connected World* (1st edn, Random House 2001).
[55]Daniel Solove, '*The Future of Reputation: Gossip, Rumor and Privacy on the Internet*' (Yale University Press 2007) 4.
[56]Yaman Akdeniz, 'Governance of Pornography and Child Pornography on the Global Internet: A multi layered approach, in law and in the internet' (1997) Regulating Cyberspace 223.
[57] Maria Murphy & Rónán Kennedy, *Information and Communications Technology Law in Ireland* (1st edn Clarus Press 2017)165.
[58] Pauline Walley, 'In Memory Amore: Revenge, Sex and Cyberspace' (2015) 20(2) The Bar Review 33.
[59] ibid.

law.[60] Competition law in America demonstrates another example of the conflict and challenge between old ways of regulating and new ways of conducting business. In a US case against Microsoft, Judge Jackson recognised that antitrust law would need to adapt to some degree to take into account considerations such as those that arise when a firm technologically ties its products to disadvantage a competitor or respond to strong network effects.[61] The above examples show how law must evolve when current law fails to achieve its goals in the online context. Challenges remain when applying targeted laws to the internet as 'new laws' designed for the current technological context must keep up with emerging developments that may bring new legal challenges.

Jurisdiction

> 'A state may not exercise its power in any form in the territory of another state'[62]

In the 'real' world, laws are designed to protect physical goods and to control the actions of corporeal individuals.[63] This protection is carried out through the concept of jurisdiction. Jurisdiction establishes boundaries that determine the law to be followed by those entering beyond that boundary. Schiff Berman describes jurisdiction by stating 'nation-states exist in autonomous, territorially-distinct, spheres and that activities therefore fall under the legal jurisdiction of only one legal regime at a time'.[64] Miller suggests jurisdiction exists in three forms: jurisdiction to prescribe, to adjudicate, and to enforce.[65] Jurisdiction can be defined as territorial borders separating countries into distinct entities marked with laws that are used to resolve a conflict.[66] However, what happens if there is no physical border? Jurisdictional problems come to the forefront of a conflict when a legal dispute occurs in a world without clearly defined borders. The internet provides an 'information superhighway' that is accessible in any place in the world notwithstanding the potential for geo-blocking[67] and government censorship. The

[60] Pauline Walley, 'In Memory Amore: Revenge, Sex and Cyberspace' (2015) 20(2) The Bar Review 33.
[61] Amicus Curiae v Microsoft [1999] D.D.C Civ 98 – 1232.
[62] S.S. 'Lotus', France V Turkey, Judgement, (1927) PCIJ Series A no 10, ICGJ 248.
[63] Andrew Murray, *Information Technology Law: The law and Society* (2nd edn., Oxford University Press 2010).
[64] Paul Schiff Berman, *Global Legal Pluralism: A Jurisprudence of Law Beyond Borders* (Cambridge University Press 2012) 4.
[65] Samuel Miller, 'Perspective Jurisdiction over internet activity: The Need to Define and Establish the Boundaries of Cyberlibert' (2003) 10 Indiana Journal of Global Legal Studies 227.
[66] Michael Gilden, 'Jurisdiction and the Internet: The 'Real World' meets cyberspace' (2000) 7(1)*ILSA Journal of International & Comparative Law* 149.
[67] Geoblocking is technology that restricts access to Internet content based upon the user's geographical location. see Tatiana Eleni Synodinou, 'Geoblocking in EU Copyright Law: Challenges and Perspectives' (2020) 69 GRUR International, Journal of European and International IP law 136.

concept of borders can appear irrelevant to this 'superhighway'.[68] The process of digitisation and the expansion of the internet have proven to be a logistical challenge for lawmakers. Early research identified that a key regulatory challenge of the internet lies in the geography of the place, or, rather, in its lack of geography.[69] The internet has no territorially based boundaries because the cost and speed of message transmission on the internet is almost entirely independent of physical location. Therefore, the internet radically undermines the relationship between legal significance and geographical location.[70] Challenges to regulation posed by the internet are embedded in the lack of power of national governments to assert control over a territory with no boundary or connection between the online behaviour and the effects on individuals or things.[71]

However, one can argue that jurisdiction is not wholly the problem when seeking to gain control over the internet. Extraterritorial effect is a well-settled principle that permits nations to regulate conduct occurring outside their borders if that conduct has 'significant effects' within their borders. Therefore, a transaction can be regulated legitimately by the jurisdiction where it occurs and the jurisdictions where significant effects of the transaction are felt.[72] So, if an action carried out on the internet affects a person in a 'real space' territory, that territory can have jurisdiction to apply its laws due to the principle of extraterritorial effect. As a result, the issue substantially lies in enforcement.

A nation can appear to regulate activity that takes place anywhere. A territory can enact a law that appears to bind the global population.[73] Yet the scope of such a law depends on the territory's ability to enforce it. A nation can enforce its laws against people with a

[68]Michael Gilden, 'Jurisdiction and the Internet: The 'Real World' meets cyberspace' (2000) 7(1)*ILSA Journal of International & Comparative Law* 149.

[69] David R. Johnston & David G. Post, 'Law and Borders – The rise of Law in Cyberspace' (1996) 48 Stanford Law Review 1367; Andrew Murray, 'Nodes and Gravity in Virtual Space' (2011) 5 *Legisprudence* 195.

[70] David R. Johnston and David G. Post, 'Law and Borders – The Rise of Law in Cyberspace' (1996) 48 Stanford Law Review 1367.

[71] David G Post, 'Governing Cyberspace: The Law' (2008) 24 Santa Clara Computer & High Tech L.J 883. However, while Governments may in general not have control over the internet, the regaining of control is possible through extreme restrictive measures which pose major issues for free speech and democracy. An example of this is the 'Great Firewall of China' whereby the Chinese government utilises substantial technical filtering methods by blocking user access to certain websites that the government declares illegal, by openly deleting webpages and blogs, and by shutting down internet access altogether in times of social upheaval. Although the Chinese Government were initially focused on deleting or blocking specific content, mainly news and pornography, the focus shifted to also preventing and disrupting any content that went against the interests of the Government. The focus later further developed to prevent 'dissent and adjudged antisocial attitudes' from taking hold. See Richard Clayton, Steven Murdoch & Robert Watson, 'Ignoring the Great Firewall of China' In: Danezis G., Golle P. (eds) *Privacy Enhancing Technologies* (PET 2006); Marina Sechenova, 'Fahrenheit 451: burning through the great firewall of China' (2016) 3 The Indonesian Journal of International & Comparative Law: Socio-Political Perspectives.

[72] Jack L. Goldsmith, 'The Internet and the Abiding Significance of Territorial Sovereignty' (1998) 5 Indiana Journal Global Legal Studies 475.

[73] David G. Post, 'Against 'Against Cyberanarchy' (2002)17 Berkeley Technology Law Journal 1365.

presence or assets in the nation's territory, people over whom the nation can obtain personal jurisdiction and enforce a default judgment against them abroad or those whom the nation can successfully extradite.[74] A defendant's physical presence or assets within the territory remains the primary basis for a nation or state to enforce its laws. Many people who interact on the internet have no presence or assets in the jurisdictions in which their actions affect. Enforcement issues are also present as not only do the police have to be able to identify the perpetrator of the offence; they must also be able to prove their case. As a result, they need to provide the prosecution with sufficient evidence. This duty will require the use of digital forensic techniques,[75] and police forces may lack the technical ability or resources to acquire the necessary evidence in many cases. This fact was highlighted in Ireland where it has been reported that the Gardaí are ill-equipped to tackle online crime.[76]

Due to the challenges associated with jurisdiction in the digital age, international co-operation is essential to ensure the enforcement of law. The Cybercrime Convention can be regarded as a significant example of such cooperation. The Cybercrime Convention entered into force in 2004. By April 2017, 53 states had acceded to it. It creates international co-operation for the regulation of a wide variety of cybercrime issues such as publication and sharing of indecent images of children, and computer-related fraud. It has been described as 'the most comprehensive instrument in the international fight against cybercrime'.[77] While Ireland signed the Cybercrime Convention on the 28th of February 2002, Ireland has not yet ratified.[78]

Anonymity

Anonymous communication is regarded as a 'cornerstone' of internet culture.[79] Some observers have even described online anonymity as a 'strong human and constitutional

[74] ibid.
[75] Barbara Etter, 'The Forensic Challenges of E-Crime' (7th Indo-Pacific Congress on Legal Medicine and Forensic Sciences, Melbourne, 21 September 2001).
[76] Department of Communications, Climate Action and Environment, 'Open Policy Debate Online Safety' (Royal Hospital Kilmainham, 6 March 2018) 15; Policing Authority Annual Report 2018.
[77] Maria Kaiafa-Gbandi, 'Criminalizing Attacks against Information Systems in the EU: The Anticipated Impact of the European Legal Instruments on the Greek Legal Order' (2012) 20(1) European Journal of Crime, Criminal Law, and Criminal Justice 59,61.
[78] Council of Europe, 'Chart of signatures and ratifications of Treaty 185' <https://ccdcoe.org/organisations/council-of-europe/> accessed 10 January 2022.
[79] David Davenport, 'Anonymity on the Internet: Why the Price May Be Too High' (2002) 45 Communications of the ACM 33.

right'.[80] Anonymity has been defined as being 'unidentifiable within a set of subjects'.[81] Rao and Rohatgi describe anonymity as the ability of an individual to perform a single interaction with another entity (or set of entities), without leaking any information about his/her identity.[82] According to Marx, a person is regarded as anonymous if (s)he cannot be identified according to any of the seven dimensions of identity knowledge.[83] These seven dimensions include: legal name, location, pseudonyms that can be linked to the person's legal name or location, pseudonyms that cannot be linked to specific identity information but that provide other clues to identity, revealing patterns of behaviour, membership in a social group, or information, items, or skills that indicate personal characteristics.[84] Anonymity from an online perspective simply means that the real author of the message or communication is unknown and cannot be identified. A related but distinct concept is pseudonymity, where a name which is not the real author's name is shown.[85] Rao and Rohatgi provide one conception of pseudonymity as enabling an individual to participate in a series of web interactions, all linkable to a single identifier (also known as a pseudonym), with the guarantee that the pseudonym cannot be linked back to the individual's identity.[86] The persistence of pseudonyms permits the establishment of long term web-relationships.[87] The ability of an individual to choose different pseudonyms for different activities enables an individual to further protect his/her privacy by partitioning his/her interactions into unlinkable activities.[88] It should be noted that in spite of the theory of pseudonymous identities, identities can often be determined through the use of additional information.

---

[80] ibid.

[81] Andreas Pfitzmann & Marit Köhntopp, 'Anonymity, Unobservability, and Pseudonymity – A Proposal for Terminology' in Hannes Federrath (ed), *Designing privacy enhancing technologies* (Springer-Verlag 2001).

[82] Josyula Rao & Pankaj Rohatgi, 'Can Pseudonymity Really Guarantee Privacy?' (9th USENIX Security Symposium Paper 2000) 85.

[83] Garry Marx, 'What's in a Name? Some Reflections on the Sociology of Anonymity' (1999) 15 The Information Society 99.

[84] ibid.

[85] Andreas Pfitzmann & Marit Köhntopp, 'Anonymity, Unobservability, and Pseudonymity – A Proposal for Terminology' in Hannes Federrath (ed), *Designing privacy enhancing technologies* (Springer-Verlag 2001). This is distinct from the concept of 'pseudonymisation' as defined in the GDPR. Article 4(5) GDPR defines 'pseudonymisation' as 'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person'.

[86] Josyula Rao and Pankaj Rohatgi, *Can Pseudonymity Really Guarantee Privacy?* (9th USENIX Security Symposium Paper 2000) 85.

[87] ibid.

[88] ibid.

Anonymity is socially useful and has been a vital tool for the preservation of political speech and discourse throughout history. As a concept anonymity is closely related to free speech and privacy. Internet technology allows anonymous communications that can be used for several purposes, including those that are socially useful and those that are criminal. Anonymity lifts inhibitions and can lead to unusual acts of kindness or generosity, or it can lead to misbehaviour and acts that are illegal or harmful.[89] Unfortunately, it is these new opportunities for criminal behaviour that cause legal issues. Kang, Brown, and Kiesler conducted a study in 2011/2012 which interviewed 44 people who had used the internet anonymously from America, Asia, Europe, and Africa about their experiences.[90] Results showed that 53% of interviewees used anonymity for illegal or malicious activities such as attacking or hacking others, or they engaged in socially undesirable activities, including browsing sites depicting violence or pornography. Other socially undesirable activities included downloading files illegally, stalking, or searching for others' personal information online.[91]

Anonymity not only allows crimes to be carried out more freely; it can also create a disconnect from the real world that fosters new perpetrators.[92] Anonymity directly creates a new breed of perpetrators, for when people believe their actions will not be attributed to them personally, they become less concerned about social conventions.[93] Essentially, these people would not carry out the act if they knew they could be identified or connected to the act. Research has shown that people, when they are hidden, tend to ignore social norms.[94] The online perpetrator can commit a crime anywhere in the world from the comfort of their own safe environment. Some people while online feel separated from the real world and disconnect their online actions from real life.[95] Physical

[89] John Suler,' The Online Disinhibition Effect' (2004) 7 Cyber psychology & behaviour 321.
[90] Ruogu Kang, Stephanie Brown and Sara Kiesler, 'Why Do People Seek Anonymity on the Internet? Informing Policy and Design' (Changing Perspectives Conference, Paris, April 2013). 'We interviewed 44 participants, 23 women and 21 men. Interviewees were from the United States (15), mainland China (14), Taiwan (9), Hong Kong (1), the Philippines (1), the United Kingdom (1), Romania (1), Greece (1), and Ethiopia (1). Their ages and occupations varied widely; there were students, employees, and retirees. Interviewees reported a range of technical computing skills from practically none to advanced; one interviewee was an IT manager and another had a university degree in network security.'
[91] Ruogu Kang, Stephanie Brown and Sara Kiesler, 'Why Do People Seek Anonymity on the Internet? Informing Policy and Design' (Changing Perspectives Conference, Paris, April 2013); Dorothy E. Denning and William E. Baugh, 'Hiding crimes in cyberspace' in D. Thomas and B. D. Loader (eds), *CyberCrime: Law Enforcement, Security, and Surveillance in the Information Age* (Routledge 2000) 105-l32.
[92] Danielle Keats Citron, *Hate Crimes in Cyberspace* (1st edn, Harvard University Press 2014) 58.
[93] Patricia Wallace, *The Psychology of the Internet* (2nd edn, Cambridge University Press 2001) 124.
[94] Arnold Goldstein, The Psychology of Group Aggression (John Wiley and Sons 2002); Brian Mullen, 'Operationalizing the Effect of the Group on the Individual: A Self-Attention Perspective' (1983) 19 Experimental Social Psychology Journal 295.
[95] Danielle Keats Citron, *Hate Crimes in Cyberspace* (1st edn, Harvard University Press 2014) 58.

separation exacerbates the tendency to act on destructive impulses. People are quicker to resort to abusive behaviour when there are no 'social cues, such as facial expressions, to remind them to keep their behaviour in check'.[96] This tendency causes severe risks since people are not aware of the extent of damage their online actions can cause to others daily in the real world. The link between the action carried out online and the possible end result in the real world is either unknown or masked and thus creates a new breed of perpetrators. This not only causes harm to the victim of the crime but also to the perpetrator themselves if their identity is revealed.

This risk is evident in the case of a 63-year-old English woman called Brenda Leyland. In 2014, Brenda sent thousands of tweets under the pseudonym '@sweepyface' stating her view, in an angry and outspoken manner, that the parents of the missing child Madeline McCann were involved in the child's disappearance. However, offline Brenda behaved very differently to her Twitter persona. Shortly after she was publicly exposed and could no longer rely on anonymity, she committed suicide.[97] This case highlights not only how anonymity gives people courage to act in a manner they would not normally act, but also the dangers involved when anonymity is relied upon but is later taken away. Perceived anonymity may also occur whereby a person does not try to hide their identity.[98] Because online users cannot see those who they are interacting with, they 'experience their activities as though others do not know who they are'.[99] They are less self-aware because they think their actions are being 'submerged in the hundreds of other actions taking place online'.[100]

Justice requires accountability.[101] But how do we serve justice if we do not know who to punish? Resolving any unfairness requires that those responsible for the injustice are held accountable through punishment so to serve justice and deter the continuation of the behaviour. In a territory which is free and fair, justice must exist and be seen to exist.[102] This requirement creates challenges in cyberspace where anonymity hinders

---

[96] Patricia Wallace, *The Psychology of the Internet* (2nd edn, Cambridge University Press 2001) 126.
[97]Grace Dent, 'The Case of Brenda Leyland and the McCanns is a thoroughly modern tale of internet lawlessness' *The Independent* (Dublin, 6 October 2014).
[98] Danielle Keats Citron, *Hate Crimes in Cyberspace* (1st edn, Harvard University Press 2014) 59.
[99] Adam Joinson, *Understanding the Psychology of Internet Behaviour: Virtual Worlds, Real Lives* (Palgrave Macmillan 2003) 23.
[100] Katelyn McKenna & John Bargh, 'Plan 9 from Cyberspace: The Implications of the Internet for Personality and Social Psychology' (2000) 4 Personality and Social Psychology Review 60.
[101] David Davenport, 'Anonymity on the Internet: Why the Price May Be Too High' (2002) 45 Communications of the ACM 33.
[102] ibid.

accountability. If people remain anonymous, identification is unachievable and it is impossible to hold them accountable.[103] Anonymous communications on the internet open the door to many forms of criminal and anti-social behaviour, while leaving victims and society helpless, and the serving of justice impossible. However, there is the argument that the experience of being anonymous is a 'myth'.[104] All of a user's activities on the internet can be linked with a device, unless precautions such as using anonymising proxies are taken.[105] Intermediaries such as Google and Facebook, using advanced resources, have access to an enormous amount of information. With specific tools, those internet companies can identify a previously anonymous person and identify his/her profile.[106]

1.3 Introducing image-based sexual abuse

IBSA typically relates to the dissemination of an intimate image without the consent of the person portrayed.[107] One of the fastest growing areas of concern in internet law is the increasing online proliferation of sexually explicit material, uploaded without the consent of the subject, often for the purpose of humiliating or blackmailing the subject.[108] IBSA has recently received extensive media attention as a 'newly minted pop culture phenomenon'.[109] While the concept of IBSA is not a novel act, advances in technology and the evolution of modern relationships have adapted and facilitated it. It is not a new phenomenon, but its prevalence, reach, and impact have increased in recent years.

1.3.1 The historical development of image-based sexual abuse

IBSA is not a new act but rather a set of behaviours that have always existed. Technology has changed the way in which these behaviours are now carried out. It is important to understand early examples of IBSA as they help demonstrate the core behaviour in its simplest form without the assistance of internet-based technology.

---

[103] ibid.
[104] Daniel Solove, 'The PII problem: Privacy and a New Concept of Personally Identifiable Information' (2011) 86 New York University Law Review 1814.
[105] Sara Nogueira Silva & Chris Reed, 'You can't always get what you want: Relative anonymity in cyberspace' (2015) 12(1) ScriptED< > (accessed 27 October 2022).
[106] ibid.
[107] Pauline Walley, 'In Memory Amore: Revenge, Sex and Cyberspace' (2015) 20(2) The Bar Review 33.
[108] ibid.
[109] Aaron Sankin, 'Revenge Porn: California Legislators Go After Troubling New Trend' *Huffington Post* (San Francisco, 21 June 2013).

(i) The 'peeping Tom'

The concept of exposing a person's private intimate moments is evident as far back as early history in c.484–c.425B.C. The historian Herodotus gives the account of King Candaules whereby the King betrays his wife's trust and privacy in their relationship.[110] According to reports, King Candaules loved his wife and 'thought her the fairest woman in the whole world'.[111] The King created a plan to expose his wife while disrobed to boastfully display her beauty. He approached the guard Gyges to pursue his plan by ordering him to peep at his wife while naked. Gyges pleaded his reluctance, stating 'I hold thy wife for the fairest of all womankind. I beseech thee ask me not to do wicked'. Despite Gyges' hesitation the King persisted, and Gyges participated. While this example did not involve any recording, it illustrates the point that the underlying behaviours and inclinations that may lead a person to engage in IBSA have predated the existence of the enabling technologies.

(ii) Mapping the camera's development

Until the late nineteenth century, paintings were the predominant representation of the nude body.[112] Paintings did not capture extensive detail and therefore photography marked the beginning of a new era of visibility and facilitated the desire for 'intensive seeing'.[113] The invention of the camera allowed IBSA to develop further, assisting in capturing the event. The concept of a device which would capture a moment was first mentioned by physicist Ibn al-Haytham in his book 'Book of Optics' in 1021.[114] In 1816 the first camera image was created by Nicephore Niepce. George Eastman further developed the concept with his invention of the photographic film, which he called the Kodak.[115] By 1900, the camera was popularised with the Brownie box camera.[116] The industrialisation of camera technology enabled the accessibility of all visual experiences

[110] Herodotus, 'The memos of Herodotus' in Robert Hutchins and George Rawlinson (eds), *Great Books of the Western World: Herodotus* (1952).
[111] ibid.
[112] Chrissy Thompson & Mark A. Wood, 'A Media Archaeology of the Creepshot' (2018) 18(4) Feminist Media Studies 560.
[113] John Berger, *Ways of Seeing* (London: Viking Books 1972).
[114] Abdelghani Tbakhi & Samir Amr, 'Ibn Al-Haytham: Father of Modern Optics' (2007) 27(6) Ann Saudi Med 464; Beaumont Newhall, *The History of Photography: From 1839 to the Present* (The Museum of Modern Art 1982).
[115] Beaumont Newhall, *The History of Photography: From 1839 to the Present* (The Museum of Modern Art 1982).
[116] ibid.

by translating them into images,[117] and so the concept of capturing moments became a common practice. The 'representational possibilities' and 'mass proliferation of photographic images' became key features of modern culture due to the development of the camera.[118]

The capabilities of the camera have also evolved. One of the most important advances is the fundamental shift in both distance and proximity. The camera allows vision to be extended in ways that are inaccessible to the naked eye and, like the microscope, allows a close examination of things at a resolution that is beyond ordinary perception, thus capturing the world in new ways.[119] Consequently, the line between the private and public has become blurred.[120] People's intimate moments have been made accessible to outsiders and images can now be taken covertly. With the continual development of technology, cameras have become inexpensive, easily accessible, covert and mobile.[121] The incorporation of the camera into mobile phones has also expanded the use and popularity of the camera. Prior to the development of the camera, people who wanted to view a person's intimate areas were limited to doing so through unaided vision and capturing technology. Today, perpetrators are armed with equipment that facilitates their objectifying behaviour in different ways, enabling a degree of discretion and secrecy that was previously unattainable.[122] An experience of Marilyn Monroe dating back to the 1950s exemplifies this point.

In 1949, Monroe was financially struggling and consequently consented to pose naked for a photographer for fifty dollars.[123] By 1952, the explicit images were made public and jeopardised her evolving career.[124] Monroe's story shows how the camera and media print were used to carry out an act of IBSA. While Monroe was able to use her fame to dissolve the situation, other victims may not have been as lucky. Unlike in the case of Gyges who

---

[117] Susan Sontag, *On Photography* (New York: Picador 1977).
[118] Tim Dant & Graeme Gilloch, 'Pictures of the Past: Benjamin and Barthes on Photography and History' (2002) 5(1) European Journal of Cultural Studies 5.
[119] Chrissy Thompson & Mark A. Wood, 'A Media Archaeology of the Creepshot' (2018) 18(4) Feminist Media Studies 560.
[120] William Staples, *Everyday Surveillance: Vigilance and Visibility in Postmodern Life* (Lanham: Rowman & Littlefield 2013).
[121] Clay Calvert & Justin Brown, 'Video Voyeurism, Privacy, and the Internet: Exposing Peeping Toms in Cyberspce' (2000) 18 Cardozo Arts & Entertainment Law Journal 469.
[122] Chrissy Thompson & Mark A. Wood, 'A media archaeology of the creepshot' (2018) 18(4) Feminist Media Studies 560.
[123] Samantha H. Scheller, 'A picture is worth a thousand words: The Legal Implications for Revenge Pornography' (2015) 93 North Carolina Law Review 551,556.
[124] Margot A. Henriksen, 'Marilyn Monroe' (*American National Biography Online,* February 2000) <http://www.anb.orglarticles/18/18-00856.html.> accessed 15 August 2017.

saw the Queen disrobed, the camera allowed for a record of the event to distribute to a wider audience at a later time.

While the camera provided a means for obtaining an intimate image, the printing press provided a method for its dissemination. In the 1980s, Hustler magazine started placing sexually explicit photographs of women in its magazine, not always with the consent or knowledge of the depicted individuals. It published 'Beaver Hunt' whereby subscribers could send in pictures of nude amateur models and receive payment if the image was chosen to feature in the magazine. LaJuan Wood became one of the first known victims of IBSA when a neighbour covertly took a picture of her topless while she was on a camping trip and sent them to Hustler, exposing her body to the readers of the magazine.[125]

(iii) Self-produced erotic/ 'real core' online pornography

Today's IBSA, which uses the internet as its platform, has roots in amateur internet pornography.[126] This type of pornography began to surface in 2000 when researcher Sergio Messina highlighted a trend among individuals sharing 'self-produced erotica' in the form of photos and videos in global discussion groups.[127] Messina described this imagery as 'real core' pornography.[128] Messina distinguished real core pornography from commercial pornography on the basis that real core involved individuals' 'real unpaid sexual encounters'.[129] Real core pornography assisted the development of IBSA, popularising the concept of recording real sexual experiences. Unlike consensual real core pornography, which holds ethical principles in production and consensual imperatives in distribution,[130] IBSA disregards these elements. This development of free online sexual sharing has been a key component in the development of IBSA.

(iv) The internet, smart phones and technology

As shown, IBSA is not a new act; rather, it is an act that has been facilitated by technology. In the age of the internet, a perpetrator of IBSA may instantly spread images

---

[125] *Wood v Hustler Magazine* [1984] 736F.2D 1084, 1086 (5th Cir.).

[126] Samantha H. Scheller, 'A Picture is worth a thousand words: The Legal Implications for Revenge Pornography' (2015) 93 North Carolina Law Review 551,559.

[127] Luca Celada, 'REALCORE Sergio Messina: The Margaret Mead of Internet Porn' (*Artillery*, January 2010), <http://www.artillerymag.com/archives/v4i3-l0/current/featurel.html > accessed 15 August 2017.

[128] Simon Hardy, 'The New Pornographies: Representation or Reality?' in Fiona Attwood (ed.) *Mainstreaming Sex: The Sexualization of Western* (IB Tauris & Co 2009) 3-18.

[129]Luca Celada, 'REALCORE Sergio Messina: The Margaret Mead of Internet Porn' (*Artillery*, January 2010), <http://www.artillerymag.com/archives/v4i3-l0/current/featurel.html > accessed 15 August 2017.

[130] Ruth Barcan, 'In the Raw: 'Home-made' Porn and Reality Genres' (2002) 3(1) Journal of Mundane Behaviour.

to an audience many magnitudes larger than that possible using traditional media such as pornographic magazines.[131] The internet is a 'force multiplier', making previously private material publicly and internationally available.[132] These images can be anonymously uploaded to hundreds of sites or downloaded to an individual's personal computer within seconds. The evolution of the internet has exposed and aggravated this crime. [133] Smartphones have changed the way in which society interacts with technology, resulting in the internet being an essential part of everyday life.[134] Furthermore, smartphones have impacted the pornography industry by altering the way consumers choose to watch pornography.[135] The combination of technological advancements such as the smartphone, easy accessibility due to the internet, and the do-it-yourself (DIY) porn trend from the 2000s has led to the rise in the 'revenge porn' subcategory of pornography.[136]

Websites and blogs dedicated to IBSA started to emerge in 2008.[137] Until 2009, IBSA was not recognised as an explicit criminal offence in any jurisdiction. The internet's influence and technology's expansion of IBSA prompted the Philippines to criminalise the act in 2009[138] and New Zealand to impose the first custodial sentence for posting intimate images without consent in 2010.[139] The internet facilitated the development of the notorious IBSA-specific website called 'IsAnyoneUP.com' in 2010. It was a major development for IBSA as the website provided a popular 'go-to' platform for perpetrators to publish the material and subsequent perpetrators to view and trade images. Although this website was shut down in 2012, its creation encouraged the rise of the 'revenge porn' genre as a staple in the pornography industry with at least 3,000 pornography websites globally featuring the 'revenge porn' genre.[140] The 2014 celebrity Apple iCloud hacking

---

[131] Sam Elliott, 'Non–Consensually Shared Photography and the Need for Reform in Ireland' (2015) < https://acjrd.ie/images/PDFs/essay-competitions/Non-consensually_shared_pornography_and_the_need_for_reform_in_Ireland.pdf> accessed 20 February 2022.
[132] Michael Salter & Thomas Crofts, 'Responding to revenge porn: Challenging online legal impunity' in Comella, L. and Tarrant, S. (eds.) *New views on pornography: Sexuality, politics and the law* (Praeger Publisher: Westport 2015).
[133] Taylor Gissell, 'Felony Count 1: Indecent Disclosure' (2015) 53(1) Huston Law Review 274.
[134] Amanda Lenhart & Maeve Duggan, 'Couples, the Internet, and Social Media' (PEW Research Centre 202.419.4500 — February 2014).
[135] Taylor Linkous, 'It's Time for Revenge Porn to Get a Taste of Its Own Medicine: An Argument for the Federal Criminalization of Revenge Porn' (2014) 20 Richmond Journal of Law and Technology 14.
[136] Vanessa Nicholle Griffith, 'Smartphones, Nude Snaps, and Legal Loopholes: Why Pennsylvania Needs to Amend its Revenge Porn Statute' (2016) 16 Journal of Technology Law and Policy 135.
[137] Mary Ann Franks, *Drafting an Effective "Revenge Porn " Law: A Guide for Legislators (*Cyber Civil Right Initiative, 2 November 2015).
[138] Anti-Photo and Video Voyeurism Act 2009, s 4.
[139] Taylor Linkous, 'It's Time for Revenge Porn to Get a Taste of Its Own Medicine: An Argument for the Federal Criminalization of Revenge Porn' (2014) 20 Richmond Journal of Law and Technology 14.
[140] Clare McGlynn & Erika Rackley, 'More than Revenge Porn: Image-Based Sexual Abuse and the Reform of Irish Law' (2017) 14 Irish Probation Journal, 38.

is another example of how IBSA can occur. It is an early example of how equipment interference (commonly known as hacking) was carried out on hundreds of victims simultaneously by stealing their intimate images. On 1st of September 2014, Jennifer Lawrence, Kate Upton, Kirsten Dunst and almost a hundred other celebrities discovered that their private, intimate images had been taken through equipment interference and published on the internet. The news of the celebrities' hacking first came to light when a '4chan' user, from an alleged underground internet ring, posted the private photos on the internet to gain bitcoins.[141] Unlike during the era of King Candaules when there was no possibility to replay or review the moment, today the distribution of an intimate image online can lead to the victim being trapped in the digital realm.

1.3.2 Defining image-based sexual abuse and its effects

IBSA involves the dissemination of an intimate image without the consent of the person portrayed.[142] There are many definitions of IBSA, all with different and varied focuses capturing a broad array of behaviours. Citron and Franks provided an early definition of IBSA as the:

> distribution of sexually graphic images of individuals without their consent. This encompasses both images taken without consent of the victim of a voyeuristic nature or otherwise and images taken consensually but later distributed without consent.[143]

Harika describes the act of IBSA as:

> the distribution of sexually graphic images of individuals without their consent, specifically images originally obtained within the context of a private or confidential relationship and later distributed without consent.[144]

Bothamley and Tully have also highlighted this relationship factor by describing IBSA in the context of 'relationship breakdown'.[145] Humbach's definition encompasses:

> sexually explicit photos and videos that are posted online or otherwise disseminated without the consent of the persons shown, generally in retaliation for a romantic rebuff.[146]

---

[141] Christopher Satti, 'A Call to (Cyber) Arms: Applicable Statutes and Suggested Courses of Action for the Celebrity iCloud Hacking Scandal' (2016) 34 Quinnipiac Law Review 561.
[142] Pauline Walley, 'In Memory Amore: Revenge, Sex and Cyberspace' (2015) 20(2) The Bar Review 33.
[143] Danielle Citron & Mary Franks, 'Criminalizing Revenge Porn' (2014) 49 Wake Forest Law Review 34.
[144] Aysegul Harika, 'Banning Revenge Pornography: Florida' (2014) 39 Nova Law Review 65.
[145] Sarah Bothamley & Ruth J. Tully, 'Understanding Revenge Pornography: Public Perceptions of Revenge Pornography and Victim Blaming' (2017) 10(1) Journal of Aggression, Conflict and Peace Research.
[146] John Humbach, 'The Constitution and Revenge Porn' (2014) 35 Pace Law Review 215.

One of the first judges to provide a definition of IBSA was Mitchell J in the Australian case of *Wilson v Ferguson* where Mitchell J describes IBSA as occurring where:

> the image is typically taken by the offender with the consent of the victim or taken by the victim and then provided to the offender as part of a not uncommon contemporised practice of couples engaging in intimate communications often involving sexual images by electronic means. However, in some cases the image may have been taken surreptitiously without the victim's consent.[147]

Henry, Flynn and Powell provide an updated and more comprehensive definition of IBSA, stating that:

> image-based sexual abuse refers to the non-consensual recording, distribution, or threat of distribution, of nude or sexual images. It can include: images obtained (consensually or otherwise) in a relationship; photographs or videos of sexual assault; images obtained from the use of hidden devices to record another person (including 'upskirting' and 'down-blousing'); stolen images from a person's computer or storage device; and sexually explicit images that have been digitally altered.[148]

While the basic act or necessary element is the obtaining or dissemination of an intimate image or video without the consent of the victim, the circumstances of obtaining, distributing and motivation underlying a specific incident of IBSA may vary indefinitely.[149] The comprehensive definition set out above as provided by Henry, Flynn and Powell is adopted for the purposes of this thesis.[150]

An intimate image typically includes 'nude, semi-nude, sexual or sexually explicit images'.[151] It may also include images of a person engaged in sexual intercourse or a sexual act, wearing underwear, wearing a provocative ensemble or posed in a sexual manner whether nude, semi-nude or fully clothed.[152] Images which are aimed at

---

[147] *Wilson v Ferguson* [2015] WASC 15.

[148] Nicola Henry, Asher Flynn, & Anastasia Powell, 'Policing Image-Based Sexual Abuse: Stakeholder Perspectives' (2018) 19(6) Police Practice and Research 565.

[149] Amanda Levendowski, 'Using Copyright to Combat Revenge Porn' (2014) NYU Journal of Intellectual Property and Entertainment Law 422.

[150] Nicola Henry, Asher Flynn, & Anastasia Powell, 'Policing Image-Based Sexual Abuse: Stakeholder perspectives' (2018) 19(6) Police Practice and Research 565; Walter DeKeseredy & Martin Schwartz, 'Thinking Sociologically about Image-Based Sexual Abuse: The Contribution of Male Peer Support Theory' (2016) 2(4) Sexualization, Media, & Society; Clare McGlynn & Erika Rackley, 'Image-based sexual abuse' (2017) 37(3), Oxford Journal of Legal Studies 534; Clare McGlynn & Erika Rackley & Ruth Houghton, 'Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse' (2017) 25(1) Feminist Legal Studies 25; Anatasia Powell & Nicola Henry, 'Technology-Facilitated Sexual Violence Victimization: Results from an Online Survey of Australian Adults' (2016) Journal of Interpersonal Violence; Anatasia Powell & Nicola Henry, *Sexual violence in a digital age 'Sexual violence in a digital age'* (1st edn, Palgrave Macmillan, 2017); Anatasia Powell, Nicola Henry & Asher Flynn, 'Image-based sexual abuse' In W. S. DeKeseredy, C. M. Rennison, & A. K. Hall-Sanchez (eds.). *The Routledge International Handbook of Violence Studies* (Routledge 2018) 305-315.

[151] Nicola Henry, Asher Flynn, & Anastasia Powell, 'Policing Image-Based Sexual Abuse: Stakeholder Perspectives' (2018) 19(6) Police Practice and Research 565.

[152] Harassment Harmful Communications and Digital Safety Bill 2017, s 2.

stimulating arousal may also be included. The explicit material may be a photograph, video or audio clip.[153]

IBSA has been described as being part of a concept known as 'technology-facilitated sexual violence'.[154] 'Technology-facilitated sexual violence' is an umbrella term coined by Henry, Flynn and Powell that describes a range of sexually aggressive behaviours that are perpetrated with the aid or use of digital communication technologies.[155] Henry, Flynn and Powell break down 'technology-facilitated sexual violence' into three broad categories: technology-enabled sexual aggression, where technology is used to carry out a sexual assault; online sexual harassment, including sexual solicitation, gender-based hate speech, and image-based harassment (e.g., sending 'dick pics'); and IBSA, including the non-consensual creation, distribution, and threat to distribute, intimate images.[156] Although IBSA is a 'continuum'[157] of sexually abusive behaviours, McGlynn, Rackley, and Houghton have identified common elements including that the images are sexual in nature, perpetration is predominantly by men and women are the predominate victims, the harassment and abuse are of a sexualised nature, fundamental rights to dignity, sexual autonomy and sexual expression are breached through the harms involved , and there is a minimisation of these forms of abuse in public discourse, law and policy.[158] While all forms of IBSA share a common sexual, sexualised and abusive essence or character, they are perpetrated in a wide variety and growing number of guises.[159] Henry, Flynn and Powell break down IBSA into 3 'interrelated behaviours' including intimate images taken or created without consent, intimate images shared or distributed without consent, and threats to create or share intimate images[160]

1. <u>Intimate images taken or created without consent</u>

[153] Pauline Walley, 'In Memory Amore: Revenge, Sex and Cyberspace' (2015) 20(2) The Bar Review 33.
[154] Nicola Henry, Asher Flynn, & Anastasia Powell, 'Policing image-based sexual abuse: stakeholder perspectives' (2018) 19(6) Police Practice and Research 565.
[155] Anastasia Powell and Nicola Henry, *Sexual violence in a digital age* (Palgrave Macmillan 2017).
[156] Nicola Henry, Asher Flynn, & Anastasia Powell, 'Policing image-based sexual abuse: stakeholder perspectives' (2018) 19(6) Police Practice and Research 565; Anastasia Powell, Nicola Henry & Asher Flynn, 'Image-based sexual abuse' in W. S. DeKeseredy & M. Dragiewicz (eds.) *Handbook of critical criminology* (NY: Routledge 2018). Anastasia Powell and Nicola Henry, *Sexual violence in a digital age* (Palgrave Macmillan 2017).
[157] Clare McGlynn, Erika Rackley and Ruth Houghton, 'Beyond 'Revenge Porn': The Continuum of Image Based Sexual Abuse' (2017) 25 Legal Studies 25; Nicola Henry, Asher Flynn, & Anastasia Powell, 'Policing image-based sexual abuse: stakeholder perspectives' (2018) 19(6) Police Practice and Research 565.
[158] Clare McGlynn, Erika Rackley and Ruth Houghton, 'Beyond 'Revenge Porn': The Continuum of Image Based Sexual Abuse' (2017) 25 Legal Studies 25.
[159] ibid.
[160] Nicola Henry, Asher Flynn, & Anastasia Powell, 'Policing image-based sexual abuse: stakeholder perspectives' (2018) 19(6) Police Practice and Research 565.

The non-consensual taking or creation of intimate images captures situations where a person is photographed or filmed without their consent, in public and/or private settings.[161] It includes content covertly recorded by an ex-partner, current partner, known party (such as a friend) or an unknown third party. [162] This form of IBSA can involve the secret filming of sexual encounters in intimate relationships, sometimes in the context of domestic violence or the secret filming in homes, changing rooms, hotel rooms or public places by known or unknown third parties.[163] Another term used for this form of observing, tracking and recording of intimate activities and bodies is digital voyeurism.[164] A slang term that has been adopted to describe this behaviour of surreptitiously capturing intimate images and then often distributing without consent is 'creepshotting'.[165] McGlynn and Rackley describe 'creepshotting' as a 'media-friendly moniker'[166] which is a 'harmful iteration of IBSA'.[167] Other slang terms that describe sub-categories of creepshotting are 'up-skirting' or 'down-blousing'. These terms describe the secret recording of (primarily) women's breasts (down-blousing) or genitals (up-skirting) in public spaces.[168] Shoes with cameras or watches with micro-lenses are used to aid this behaviour.[169] One Australian survey found that 1 in 5 respondents had experienced this form of IBSA.[170] The taking or creation of intimate images can also include photoshopped (digitally altered) images, deep fakes and hacked images. [171] Photoshopping in this context involves transposing a victim's face onto a sexually explicit body.[172] Further developments in technology have led to 'deep fakes' whereby machine-learning

[161] Nicola Henry, Asher Flynn, & Anastasia Powell, 'Policing image-based sexual abuse: stakeholder perspectives' (2018) 19(6) Police Practice and Research 565.
[162]Pauline Walley, 'In Memory Amore: Revenge, Sex and Cyberspace' (2015) 20(2) The Bar Review 33.
[163] See for example Welsh v. Martinez, 144 A. 3d 1231 (Conn. App. Ct. 2015). The defendant gave the plaintiff gifts for her bedroom, including a clock radio that contained a spy camera.
[164] Danielle Citron, 'Sexual Privacy' (2019) 128(7) The Yale Law Journal 1870.
[165] Chrissy Thompson & Mark A. Wood, 'A media archaeology of the creepshot' (2018) 18(4) Feminist Media Studies 560.
[166] Clare McGlynn and Erika Rackley, 'Image-Based Sexual Abuse' (2017) 37(3) Oxford Journal of Legal Studies 534.
[167] ibid.
[168] Clare McGlynn & Erika Rackley, 'Image-Based Sexual Abuse: More than just 'Revenge Porn'' (2016) Research Spotlight.
[169] Alisdair A. Gillespie, '"Up-Skirts" and "Down-Blouses:" Voyeurism and the Law' (2008) Criminology Law Review 370.
[170] Nicola Henry, Anastasia Powell & Asher Flynn, *Not just 'revenge pornography': Australians' experiences of image-based abuse: A summary report* (Melbourne: RMIT University 2017). This included 1 in 10 (10.2%) women who reported 'downblousing' and 1 in 20 (5.6%) women who reported 'upskirting.' Only respondents who became aware that someone had filmed them could report these experiences.
[171]Amanda Levendowski, 'Using Copyright to Combat Revenge Porn' (2014) NYU Journal of Intellectual Property and Entertainment Law 422.
[172] ibid.

technologies are being used to create 'deep fake' sexual content where people's faces and voices are transposed onto pornography.[173]

2. Intimate images shared or distributed without consent

A particularly harmful form of IBSA is the non-consensual sharing or distribution of intimate images.[174] The act of disseminating intimate images mainly occurs via the internet through social media, email, pornography websites or 'revenge pornography'-specific websites. One Australian survey found that 1 in 10 respondents had experienced this form of IBSA.[175] The disseminated material may have been generated consensually either jointly with another person or taken by oneself and initially shared in a limited fashion to a chosen audience, often of one other person.[176] The harm occurs when the images are shared beyond the intended audience without the consent of the subject of the image. The disseminated images may also have been covertly recorded. Once the intimate images have been shared online, it becomes a challenge for the victims to regain control of their images and to remove them from the online sphere.[177] Disseminated images are often accompanied by the victim's personal information, such as their contact details. The addition of this personal information adds another dimension to the behaviour as it encourages cyber harassment and cyber-stalking.[178] Victims not only seek to regain control of their images but remain fearful for their safety in the offline world. [179] Possible motivations include spite or personal entertainment.[180] Perpetrators may, for example, distribute intimate images for sexual gratification and/or to boost social status among a closed and secret group.[181] Acts of publishing IBSA may also be motivated by a commercial incentive to extort or generate money.[182] 'Sexploitation' is a term that is used

[173] Danielle Citron, 'Sexual Privacy' (2019) 128(7) The Yale Law Journal 1870.
[174] Nicola Henry, Asher Flynn & Anastasia Powell, 'Policing Image-Based Sexual Abuse: Stakeholder Perspectives' (2018) 19(6) Police Practice and Research 565.
[175] Nicola Henry, Anastasia Powell & Asher Flynn, *Not Just 'Revenge Pornography': Australians' Experiences of Image-Based Abuse: A Summary Report* (Melbourne: RMIT University 2017); Kathryn Branch, Carly M. Hilinski-Rosick, Emily Johnson, & Gabriela Solano, 'Revenge Porn Victimization of College Students in the United States: An Exploratory Analysis' (2017) 11(1) International Journal of Cyber Criminology 128.
[176] Sexting involves the sending of sexually explicit messages or images via a device or over the internet. Theresa Senft & Nancy Baym, 'What Does the Selfie Say? Investigating a Global Phenomenon' (2015) 9 International Journal of Communication1588.
[177] Danielle Keats Citron, *Hate Crimes in Cyberspace* (1st edn, Harvard University Press 2014).
[178] ibid.
[179] Nia Bahadue, 'Victims of Revenge Porn Open Up on Reddit about How It Impacted Their Lives', *Huffington Post* (New York, 10 January 2014).
[180] James Dawkins, 'A Dish Served Cold: The Case for Criminalizing Revenge Pornography' (2015) 45 Cumberland Law Review 395.
[181] Nicola Henry, Asher Flynn & Anastasia Powell, 'Policing Image-Based Sexual Abuse: Stakeholder Perspectives' (2018) 19(6) Police Practice and Research 565.
[182] John Humbach, 'The Constitution and Revenge Porn' (2014) 35 Pace Law Review 215.

to refer to the commercial exploitation of sex or sexually explicit material in the media (such as film, advertising and other mass media).[183] Hunter Moore's website 'IsAnyoneUp.com' featured intimate images of people and published personal details alongside these images. This site generated $8,000 to $13,000 per month in advertising revenue.[184] However, Moore boasted that this figure sometimes reached $30,000 in a month.[185]

3. Threats to create or share intimate images

In 2013, the internet security company McAfee conducted an online survey of customers and found that one in ten adults had been threatened by an ex-partner to release intimate images.[186] Some reports suggest that some perpetrators coerce victims into taking images of themselves or having the images being taken of them; or threaten to distribute images to force the victim to engage in an unwanted act, perform a sexual act, or preventing the victim from leaving a relationship.[187] A friend, partner, rapist, sex trafficker or abuser may also threaten the act or perpetrate the act itself to blackmail the victim.[188] This blackmail may occur to extort money, control a relationship or extort further intimate images. Sextortion is a relatively new term used to describe an act of IBSA where a perpetrator obtains intimate images of a victim and then threatens to distribute those images unless the victim sends them further intimate images.[189]

IBSA - whether carried out by an ex-partner, hacker, friend, abuser or unknown third party - is not just one behaviour of publishing an intimate image but a cluster of

[183] Anastasia Powell and Nicola Henry, *Sexual Violence in the Digital Age* (Palgrave Macmillan: London 2017) 128.
[184] Kashmir Hill, 'Revenge Porn with a Facebook Twist' (Forbes, 6 July 2011) < https://www.forbes.com/sites/kashmirhill/2011/07/06/revenge-porn-with-a-facebook-twist/?sh=1abc8a2e1d2e > accessed 20 February 2022; Kashmir Hill, 'Why we find Hunter Moore and his "identity porn" site, IsAnyoneUp, so fascinating' (Forbes , 5 April 2012) < https://www.forbes.com/sites/kashmirhill/2012/04/05/hunter-moore-of-isanyoneup-wouldnt-mind-making-some-money-off-of-a-suicide/?sh=e4ed0ef794be > accessed 20 February 2022; Scott R. Stroud, 'The Dark Side of the Online Self: A Pragmatic Critique of the Growing Plague of Revenge Porn' (2014) 29 Journal of Mass Media Ethics 168.
[185] Alex Morris, 'Hunter Moore: The most hated man on the internet' (Rolling Stone, 11 October 2012) < https://www.rollingstone.com/culture/culture-news/hunter-moore-the-most-hated-man-on-the-internet-184668/ > accessed 20 February 2022; Scott R. Stroud, 'The dark side of the online self: A pragmatic critique of the growing plague of revenge porn' (2014) 29 Journal of Mass Media Ethics 168.
[186] McAfee, 'Lovers beware: scorned exes may share intimate data online' (2013) <www.mcafee.com/us/about/news/2013/q1/20130204-01.aspx >accessed 20 February 2022.
[187] Nicola Henry, Asher Flynn & Anastasia Powell, 'Policing image-based sexual abuse: stakeholder perspectives' (2018) 19(6) Police Practice and Research 565.
[188] Aysegul Harika, 'Banning Revenge Pornography: Florida' (2014) 39 Nova Law Review 65.
[189] Benjamin Wittes, Cody Poplin, Quinta Jurecic, & Clara Spera, 'Sextortion: Cybersecurity, Teenagers, and Remote Sexual Assault' (Centre for Technology Innovation at Brookings — May 2016); Danielle Citron, 'Sexual Privacy' (2019) 128(7) The Yale Law Journal 1870; Anastasia Powell and Nicola Henry, *Sexual Violence in the Digital Age* (Palgrave Macmillan: London 2017).

activities that result in varying levels of harm.[190] Therefore, it is important to highlight the different ways in which this content can be published, and how it can remain linked to the victim.

The act of IBSA can be described as having four variable dimensions:

1. the source of the content posted
2. the consent-status of the material posted
3. the intent of the agent doing the posting
4. identifying features in the content [191]

These dimensions are presented in the table below:

Content Source	**Content Status**	**Poster Intent**	**Identifying Content**
Self	Granted	Praise subject	Known identifiers
Other	Not granted	Harm subject	Unknown identifiers
Online	Uncertain	Other intentions	No possible identifiers

Figure 1 Types of Revenge/Nonconsensual Porn Posting Behaviours[192]

The first dimension of posting behaviour involves the establishment of the origin of the content before it is disseminated. It needs to be established whether the content came from the actions of the poster, i.e., the person who posts the material, or whether another party sent it to them. The source dimension can be divided into 'poster-created' and 'other-created' content.[193] The category of 'other-created' content includes content sent from a partner, friend or hacker, as previously mentioned. However, it could also be content that was stumbled upon online, in which case the authorship of the material is unclear. For

[190] Scott Stroud, 'The Dark Side of the Online Self: A Pragmatist Critique of the Growing Plague of Revenge Porn' (2014) 29 Journal of Mass Media Ethics 168.
[191] Scott Stroud & Johnathan Henson, 'Social Media, Online Sharing and the Ethical Complexity of Consent in Revenge Porn' In A. Close (ed.), *Online Consumer Behavior: The Dark Side of Social Media* (United States: Routledge Press 2017).
[192] ibid.
[193] Scott R. Stroud, 'The Dark Side of the Online Self: A Pragmatist Critique of the Growing Plague of Revenge Porn' (2014) 29 Journal of Mass Media Ethics 168.

example, a person could use a search engine to search a term and come across an explicit image. Certain factors about this image are necessarily unclear to the observer. These include: whether the image is consensual or not, the origin of the image, whether the person in the image is a victim or whether they posted it themselves.

The second dimension of IBSA postings involves the consent element of the images. Although the discussion of consent generally amounts to whether consent was given or not, content can possess a range of consent-statuses.[194] The view that images simply 'come with consent or without consent' is misleading.[195] It must be considered when defining IBSA that one cannot look at an image and see the consent granted for its use. The viewer of the image is not aware of the consent element by looking at the image. Consequently, it can be hard to establish whether an image is one of IBSA or not when it is viewed online. An image can be exchanged with or without consent for further distribution. The consent status of a given image can be uncertain when found online or when the parties do not openly talk about the limits of future distribution.[196]

The third dimension that varies according to individual posting behaviours is the intention of the post. Much of the relevant literature focuses on the intent to harm, shame or extort money. However, the possibility that someone has posted material to praise the subject, either in their actions, character, or more likely, physical appearance, is not widely considered.[197] The subject may have alluded to how much they liked the picture and are happy with their appearance in it. The image is then posted without consent, but is done so to praise, rather than to humiliate, the victim. However, there is a strong argument that the intention of the perpetrator is irrelevant as it does not affect the harm caused to the victim.[198]

The fourth dimension considers whether the victim can be identified in the image. The greater the identification of the victim in the image, the greater the potential harm. Therefore, a discussion of how a victim is identified when defining an act of IBSA is crucial. In many cases, the most harmful effect of IBSA is not simply the existence of the image but rather that the individual can be recognised as the person in the image by others

[194] Scott R. Stroud, 'The Dark Side of the Online Self: A Pragmatist Critique of the Growing Plague of Revenge Porn' (2014) 29 Journal of Mass Media Ethics 168.
[195] ibid.
[196] ibid.
[197] ibid.
[198] Mary Ann Franks, *Drafting an Effective 'Revenge Porn' Law: A Guide for Legislators* (Cyber Civil Right Initiative, 2 November 2015) *3.*

who view it.[199] These identifying factors can take many forms which do not always relate to the physical face of the victim in the image. They can include a range of typed information about the subject: first name, first name with last initial, full name, address, town, email address, employer's address or contact information, and even their phone number. These pieces of information can be called known identifiers since they are attached to the image and connect the visual depiction to an identifiable individual. Another way in which a person may be identified is through comments that may be attached to the image. The image alone may not fully identify the victim, but comments and conversations accompanying the image may confirm the identity of the victim.

Another form of identifiers is objects in the background. It may include a picture on the wall behind the victim, a certificate with a name in the image or a setting such as a college apartment. Specific marks on the person in the image, such as distinctive tattoos, piercings or birth marks, can also lead to identification. Often these marks confirm that the victim is indeed the person in the image. Therefore, someone may post an image with no typed information attached or where the victim's face is not fully visible, yet objects in the image or body marks can still enable identification.

The question arises: when is a person not identifiable in the image? One could post a photo that contains no possible identifiers; for example, in a close shot of a body part with no identifying marks or background objects visible. While the harm of invasion of privacy is still evident, harms such as stalking, the threat of physical harm or the loss of one's job are not as likely to occur. Such non-identifying shots could be used for the purposes of IBSA, but the harm element may not be as significant compared with other images that have more elaborate identifiers.

IBSA is not a single behaviour, but a variety of activities. IBSA can include the taking and/or dissemination of an intimate image or threatening to do so without the consent of the victim. Understanding this definitional scope is essential since it provides a foundation for later chapters. The above discussion of definitional scope assists the analysis process in Chapter 2 and Chapter 3 in the context of identifying the merits and limitations of laws used to combat IBSA.

[199] Scott Stroud, 'The Dark Side of the Online Self: A Pragmatist Critique of the Growing Plague of Revenge Porn' (2014) 29 Journal of Mass Media Ethics 168.

1.3.3 Image-based sexual abuse as a sexual privacy issue

Privacy has been discussed from many perspectives across many disciplines.[200] Warren and Brandeis provided an early description of privacy as the right to be 'let alone.'[201] However, privacy is a much broader concept. Westin defines privacy as 'the desire of individuals to choose freely how much of themselves to expose to others'.[202] Privacy is generally viewed as a 'multi-faceted' right that is complex, varying in nature, purpose and range, and is 'the core of individuality within the constitutional order'.[203] The importance of privacy has also been widely discussed and highlighted in academia. It has been declared as being the beginning of all freedom and the heart of liberty,[204] 'essential for the maintaining of different relationships',[205] 'crucial for the protection of autonomy'[206] and 'an integral part of humanity'.[207] The contextual nature of consent is a central concern of privacy law. Privacy laws make it clear that permitting an entity to use personal information in one context does not constitute consent to use it without the person's explicit permission in another context.[208] As has been discussed above, consent is a key factor when considering whether a behaviour amounts to IBSA. Citron defines sexual privacy as:

> The social norms that manage access to, and information about, individuals' intimate lives. This definition includes all aspects of intimate selves and activities. Sexual privacy concerns the parts of physical bodies that are closely connected to sex and gender. It involves gender and sexual identities. It includes intimate activities (including thoughts, communications and sexual behaviours) as well as the zones in which those activities occur. Sexual privacy concerns personal decisions about intimate relationships and reproductive lives.[209]

Article 8 of the European Convention on Human Rights and Article 7 of the Charter of Fundamental Rights of the European Union protect the right to respect for private life and a right to privacy is recognised as an unenumerated right under Article 40.3.1° of the Irish Constitution: 'The State guarantees in its laws to respect, and, as far as practicable, by its laws to defend and vindicate the personal rights of the citizen'.[210] The case of *McGee v*

[200] Paul M. Schwartz, 'Privacy and Democracy in Cyberspace' (1999) 52 Vanderbilt Law Review 1607.
[201] Samuel Warren & Louis Brandeis, 'The Right to Privacy' (1890) 4(5) Harvard Law Review 193.
[202] Alan Westin, *Privacy and Freedom* (New York, Atheneum, 1967) 31.
[203] *Norris v Attorney General* [1984] IR 36.
[204] *Pub. Utilities Comm'n v. Pollak,* 343 U.S. 451, 467 (1952) (Douglas, J., dissenting).
[205] James Rachels, 'Why Privacy Is Important' in Ferdinand David Schoeman (ed.) *Philosophical Dimensions of Privacy: An Anthology* (Cambridge University Press 1984) 290, 292.
[206] Beate Rössler, *The Value of Privacy* (Wiley, 2004).
[207] Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231,235 (Minn. 1998).
[208] Danielle Keats Citron, *Hate Crimes in Cyberspace* (1st edn, Harvard University Press 2014) 147.
[209] Danielle Citron, 'Sexual Privacy' (2019) 128(7) The Yale Law Journal 1870.
[210] The Irish Constitution, article 40.3.1.

Attorney General[211] established Article 40.3.1° as affording sexual privacy protection. Although this case dealt specifically with marital privacy, it highlighted how certain issues within an intimate relationship are afforded privacy protection under Article 40.3.1° European case law highlights how the term 'private life,' as protected under Article 8 of the ECHR extends to the protection of a person's autonomy, intimate moments, physical and social identity, and integrity.[212]

> The [European Court of Human Rights] . . . reiterates that 'private life' is a broad term, encompassing, inter alia, aspects of an individual's physical and social identity including the right to personal autonomy, personal development and to establish and develop relationships with other human beings and the outside world . . . furthermore, . . . the court has previously held that private life includes a person's physical and psychological integrity and that the state is also under a positive obligation to secure to its citizens their right to effective respect for this integrity.[213]

Sexual privacy entails many dimensions. Hall and Hearn suggest that sexual privacy includes informational privacy, accessibility privacy, and physical privacy.[214] Informational privacy considers a person's right to determine how, when and to what extent their information is released to others. Accessibility privacy relates to a person's right to determine how, when and to what extent their information is accessible to others. Physical privacy is the degree to which a person is physically accessible to others.[215] The dissemination of an intimate image without consent infringes on a person's right to determine who sees their personal information (that being who can see their intimate image). The posting of the image onto the internet for many people to view, download and share infringes on a person's right to control who has access to their information. Perpetrators who attach personal information about the victim under the image infringe upon their right to physical privacy as the victim may be stalked or harassed due to the release, for example, of a home address.

---

[211] *McGee v Attorney General* [1974] IR 284.
[212] *Tysiac v Poland* Application no. 5410/03 Judgment 20 March 2007 at paragraph 107, citing *Pretty v the UK* (2002) 35 EHRR para 61, *Glass v UK* Application No. 61827/00; *Sentges v The Netherlands* Application No. 27677/02 8 July 2003; *Pentiacova v Moldova* Application No. 14462/03; *Nitecki v Poland* Application No. 65653/01 21 March 2002; *Odievre v France* Application no. 42326/98, Judgment 13 February 2003.
[213]*Tysiac v Poland* Application no. 5410/03 Judgment 20 March 2007 at paragraph 107, citing *Pretty v the UK* (2002) 35 EHRR para 61, *Glass v UK* Application No. 61827/00; *Sentges v The Netherlands* Application No. 27677/02 8 July 2003; *Pentiacova v Moldova* Application No. 14462/03; *Nitecki v Poland* Application No. 65653/01 21 March 2002; *Odievre v France* Application no. 42326/98, Judgment 13 February 2003.
[214] Matthew Hall & Jeff Hearn, *Revenge Pornography Gender, Sexualities and Motivations* (Routledge: New York 2018).
[215] ibid.

1.3.4 The effects of image-based sexual abuse

IBSA can have significant and serious impacts on victims. It has been reported that victims of these attacks experience emotional distress that can result in grave consequences including suicide.[216] IBSA not only has immediate effects of humiliation, embarrassment and a sense of betrayal[217] but can also cause long-term fear and anguish, employment and educational issues,[218] interpersonal relationship destruction and complications, threat of physical harm[219] and psychological issues.[220] In 2016, Bates carried out 18 in-depth semi-structured interviews with Canadian and American adult IBSA victims who had self-identified as victims or survivors. She noted that her research participants described having experienced post-traumatic stress disorder (PTSD), anxiety, depression, and a loss of self-esteem.[221]

Once an image is uploaded, it can dominate the first few pages of an online search of a person's name. This prominence allows the image to be forever connected to the victim. The connection can lead to lost jobs and educational opportunities. In a recent study, colleges and universities revealed that they use social networking sites and Google searches as a medium to evaluate applicants and commonly come across primary and secondary sexting images which have a negative impact on the subject's application.[222] In another study conducted by Microsoft, it was discovered that 80% of recruiters conduct online searches of candidates and many of them use a range of sites, such as photo and video sharing sites, when scrutinising candidates.[223] 90% of employers conduct online searches on prospective employees, with 70% of these employers rejecting applicants due to their findings.[224] Common reasons for rejecting candidates for an interview included concerns about the applicant's lifestyle, 'inappropriate' online comments and 'unsuitable'

[216] Danielle Citron & Mary Franks, 'Criminalizing Revenge Porn' (2014) 49 Wake Forest Law Review 34.
[217] *Glynn v Minister for Justice, Equality and Law Reform* [2014] IEHC 133.
[218] Elizabeth Ryan, 'Sexting: How the State can prevent a moment of indiscretion from leading to a lifetime of unintended consequences for minors and young adults' (2010) 96 Iowa Law Review 357,363.
[219] Cyber Civil Rights Initiative, 'End Revenge Porn Infographic' (2014) <https://www.cybercivilrights.org/wp-content/uploads/2014/12/RPStatistics.pdf > accessed 20 February 2022.
[220] Danielle Citron & Mary Franks, 'Criminalizing Revenge Porn' (2014) 49 Wake Forest Law Review 34.
[221] Samantha Bates, 'Revenge porn and mental health: A qualitative analysis of the mental health effects of revenge porn on female survivors' (2016) 12(1) Feminist Criminology 22.
[222] Elizabeth Ryan, 'Sexting: How the State can prevent a moment of indiscretion from leading to a lifetime of unintended consequences for minors and young adults' (2010) 96 Iowa Law Review 357,363.
[223]Danielle Citron & Mary Franks, 'Criminalizing Revenge Porn' (2014) 49 Wake Forest Law Review 34.
[224] ibid.

photographs and videos.[225] 55% of US and 51% of UK employers have rejected candidates due to unsuitable photos.[226] Employers generally do not call victims of IBSA to interview.[227] This denial of opportunity impacts negatively on a victim's ability to secure a job, leading to financial difficulties. Explicit images can cause breakdowns in families and relationships. IBSA victims may have to endure physical harm and the threat of physical harm. 90% of victims report being stalked by others who saw their online pictures and 50% report that their contact and personal details were posted with their picture, making it easy for strangers to 'hunt them down like prey'.[228] The fear of exposure and the tension of keeping the act a secret have profound emotional repercussions.[229] The psychological effects stemming from the dissemination of a person's naked body can be significant. According to a study carried out by the Cyber Rights Initiative, over 80% of IBSA victims experience severe emotional distress and anxiety.[230] Much of this anxiety is caused by the constant fear of wondering who has viewed the image. The moment the explicit photo is posted, the idea of a permanent record of the image haunts victims. This fear was evident in the case of a US-based minor, Hope Witsell. Witsell took a topless photo of herself and sent it to another minor. The minor she sent the image to then sent the image to others and in turn they sent it to others. Witsell became a target of bullying after her school and a nearby school saw her picture. It was reported that Witsell engaged in self-harm as a result of the ordeal.[231] Witsell's subsequent suicide was attributed to the incident.[232]

Examples of image-based sexual abuse

Below are the stories of nine victims of IBSA. These cases were selected based on desk-based research. Each case highlights a different way in which the act of IBSA can occur and the various harms that can result. These case studies are selected to illustrate the

[225] Matt Ivester, *lol . . .OMG! What Every Student Needs to Know about Online Reputation Management, Digital Citizenship and Cyberbullying* (Reno, NV: Serra Knight, CreateSpace Independent Publishing Platform 2011) 95.
[226] Cross-Tab, 'Online Reputation in a Connected World' (2010) < Online Reputation in a Connected World (slideshare.net)> accessed 20 February 2022.
[227] Danielle Keats Citron, *Hate Crimes in Cyberspace* (1st edn, Harvard University Press 2014) 9.
[228] Cyber Civil Rights Initiative, 'Non Consensual Porn: A Common Offence' (*Cyber Civil Rights Initiative*, 12 June 2017) <https://www.cybercivilrights.org/2017-natl-ncp-research-results/> accessed 4 March 2019.
[229] Nicole Poltash, 'Snapchat and Sexting: A Snapshot of Baring your Bare Essentials' (2014) 19(4) Richmond Journal of Law and Technology 1.
[230] Cyber Civil Rights Initiative, 'Non Consensual Porn: A Common Offence' (*Cyber Civil Rights Initiative*, 12 June 2017) <https://www.cybercivilrights.org/2017-natl-ncp-research-results/> accessed 4 March 2019.
[231] Elizabeth Ryan, 'Sexting: How the State can Prevent a Moment of Indiscretion from Leading to a Lifetime of Unintended Consequences for Minors and Young Adults' (2010) 96 Iowa Law Review 357,363.
[232] ibid.

diverse intentions of perpetrators and the magnitude of potential harm that can be caused by IBSA.

The Irish case of 'Jane'

'Jane'[233] became a victim of IBSA when her ex-boyfriend uploaded an explicit video of them engaged in sexual intercourse, which he had covertly recorded. Along with the video he posted the words '24 year old female from Ireland who is pretty much up for anything'.[234] The Gardaí informed her that there was nothing they could do due to the lack of legislation.[235] This case highlights how victims of IBSA may receive little support from the authorities.[236]

Ugandan pop star Desire Luzinda

Desire Luzinda is a Ugandan singer and a popular figure in Uganda. Luzinda's ex-boyfriend circulated explicit pictures of her online which she had taken and sent to him during their relationship.[237] The Ugandan Ethics Minister called for her arrest for 'indecent behaviour'.[238] Statements of apology were widely expected from the victim. Luzinda stated: 'I want to sincerely apologise to my mother, to my daughter, to my family, to my friends, my fans and any other people who have been offended by these images ... I take full responsibility for having lost my mind to take such shameful pics'.[239] This case highlights the 'victim-blaming' attitude that can persist in society regarding such occurrences.

New Jersey college student Tyler Clementi

[233] This is not the victim's real name.
[234] Claire McCormack, 'Revenge Porn Nightmare: 'I felt I was Completely Violated'' *Irish Independent* (Dublin, 12 June 2016).
[235] Isabel Hayes, 'It Made me Feel Really Dirty' - Victim Powerless against Revenge Porn Attack' (*The Journal* 21 June 2016) < https://www.thejournal.ie/revenge-porn-irish-woman-no-legislation-2837138-Jun2016/ > accessed 20 February 2022.
[236] ibid.
[237] Ella Alexander, 'Ugandan Pop Star Desire Luzinda could be Arrested over 'Revenge Porn' Nude Pictures' *Independent* (12 November 2014).
[238] Gail Sullivan, 'Ugandan Official Wants to Arrest Victim of Revenge Porn: 'She Should Be Locked up and Isolated'' *Washington Post* (Washington, 12 November 2014).
[239] Ella Alexander, 'Ugandan Pop Star Desire Luzinda could be Arrested over 'Revenge Porn' Nude Pictures' *Independent* (12 November 2014).

Tyler Clementi was a student of Rutgers University, New Jersey. During his first semester he asked his roommate for some privacy in their shared room for the night as Clementi had a date who was visiting him. Clementi's roommate agreed, but set up a laptop with a camera to spy on Clementi and his date.[240] Clementi's roommate discovered that Clementi was using the room to have a sexual relationship with another man and urged his Twitter followers to watch the live stream as proof.[241] Hours after this footage was streamed, Clementi committed suicide.[242] This example demonstrates that content covertly recorded is not always recorded by an intimate partner but may also be recorded by a friend or even an unknown party. It highlights how men can also be affected by IBSA. The technology of live streaming is also a point to note as IBSA is not always an act that involves a recorded image but may also include live footage.

Celebrity hacking scandal - Jennifer Lawrence

This case occurred in 2014 when intimate images of high-profile actors, models, singers and presenters were posted online in a hacking leak linked to the Apple iCloud service.[243] The photos appeared after a user on an image-sharing forum published photographs of 101 celebrities, including Jennifer Lawrence. The images were reportedly accessed due to an iCloud leak that enabled celebrities' phones to be hacked.[244] This case demonstrates the vulnerability of celebrities (as well as the public) when taking 'selfies' and storing them on devices that could be hacked if they are not protected.

End Revenge Porn Campaign - Holly Jacobs

Holly Jacobs' case can be described as a 'typical' case of IBSA. Holly Jacobs became a victim when her ex-boyfriend posted sexually explicit pictures and videos of her online, alongside her full name, email and where she worked.[245] She and her ex-boyfriend had exchanged intimate photos throughout their relationship, but she had never anticipated that these images would become online material free for all to view. At the time, Jacobs was working towards a doctorate and fought to escape the reputational and professional

[240] Ed Pilkington, 'Tyler Clementi, Student Outed as Gay on Internet, Jumps to His Death' *The Guardian* (London, 30 September 2010).
[241] ibid.
[242] ibid.
[243] Rose Buchanan, 'Jennifer Lawrence Nude Pictures Leak Sparks Fear of More Celebrity Hackings: A Flagrant Violation of Privacy' *The Independent* (1 September 2014).
[244] ibid.
[245] Holly Jacobs, 'A Message from Our Founder' *(Cyber Civil Rights Initiative, 6 October 2013)* <http://www.cybercivilrights.org/amessagefromour_founderdrholly_.jacobs > accessed 4 March 2019.

damage that followed her online identity.[246] Her pictures were available on over 300 websites and so she was inundated with unwelcome communications from men who had viewed them.[247] After battling with pornography sites and search engines to remove her images, she had to resort to changing her name.[248] She started the End Revenge Porn Campaign and teamed up with activist Charlotte Laws and law professors Mary Anne Franks and Danielle Citron to form a non-profit organisation, the Cyber Civil Rights Initiative. This case fits the perception of what a 'typical' case of IBSA may involve, but also highlights how the attachment of personal information alongside the image can have exacerbating effects. It demonstrates how victims may never be able to detach themselves from the image and may even need to resort to changing their names.

Sex trafficked victim – 'Sarah'

'Sarah'[249] was a victim of sex trafficking. Alex Campbell used violence and force against her to perform sexual acts with another woman while he filmed it.[250] He threatened to send the recording to Sarah's family if she ever attempted to escape.[251] 'Sarah' escaped and reported Campbell to the police. He was sentenced to life imprisonment in the federal court of Chicago. This case shows how IBSA can be used as blackmail by perpetrators to gain power over others and how the production of intimate images may be coercive.

More than one perpetrator - Audrie Pott

Audrie Pott was 15 years old when she became intoxicated at a party. Three boys and a girl took her to an upstairs bedroom. After the girl left, the boys undressed Pott, drew on her body and took pictures while they sexually assaulted her.[252] The next morning, through Facebook, she realised what had happened to her and that the pictures were being

[246] Samantha H. Scheller, 'A Picture is Worth a Thousand Words: The Legal Implications of Revenge Pornography' (2014) 93 North Carolina Law Review 551.
[247] Mary Ann Franks, 'Drafting an Effective 'Revenge Porn' Law: A Guide for Legislators' (*Cyber Civil Rights Initiative*, 22 September 2016) 3 <https://www.cybercivilrights.org/wp-content/uploads/2016/09/Guide-for-Legislators-9.16.pdf> accessed 24 August 2022.
[248] ibid.
[249] This is not the victim's real name.
[250] Mary Ann Franks, 'Drafting an Effective 'Revenge Porn' Law: A Guide for Legislators' (*Cyber Civil Rights Initiative*, 22 September 2016) 3 <https://www.cybercivilrights.org/wp-content/uploads/2016/09/Guide-for-Legislators-9.16.pdf> accessed 24 August 2022.
[251] ibid.
[252] Nina Burleigh, 'Sexting, Shame and Suicide' (*Rolling Stone*, 17 September 2013) <https://www.rollingstone.com/culture/culture-news/sexting-shame-and-suicide-72148/> accessed 20 February 2022.

distributed around the school. A week later, Pott committed suicide.[253] This case shows that IBSA can have more than one perpetrator. IBSA can occur alongside other offences, in particular sexual assault.

Shaming websites - Kara Jefts

Kara Jefts is an academic living in Chicago. In 2011, Jefts ended a long-distance relationship with her boyfriend, who lived in Italy. After the breakup, explicit screenshots from their Skype conversations were released online.[254] Jefts' ex-boyfriend had emailed these images to her friends and family and had posted them to Facebook. The images were also published on websites that were devoted to exposing people with sexually transmitted diseases.[255] Jefts describes the feeling of being a victim of IBSA as being like having an 'incurable disease'.[256] This case highlights how perpetrators of IBSA may use specific websites to publish images in order to aggravate the harm, in this instance by suggesting the subject had a sexually transmitted disease.

Collateral damage – Charlotte and Kayla Laws

In 2012, Kayla Laws' Facebook and email accounts were hacked. A topless photo of Kayla Laws, along with her personal details including her name, address, Twitter handle and Facebook profile, were subsequently posted to the website 'IsAnyoneUp.com'.[257] Kayla Laws' mother, Charlotte Laws, sent the website owner, Hunter Moore, numerous takedown notices.[258] Moore refused to comply. Instead, he began targeting Charlotte Laws online and encouraged his followers to do the same.[259] The harassment took on an offline dimension when a suspicious white car parked outside their house on many occasions.[260] Charlotte Laws contacted local law enforcement and the FBI. Eventually,

[253] ibid.

[254] Charlotte Alter, 'It's Like Having an Incurable Disease': Inside the Fight Against Revenge Porn' *Time U.S* (13 June 2017).

[255] Charlotte Alter, 'It's Like Having an Incurable Disease': Inside the Fight Against Revenge Porn' *Time U.S* (13 June 2017).

[256] ibid.

[257] Carole Cadwalladr, 'Charlotte Laws' Fight with Hunter Moore, the Internet's Revenge Porn King' (*Guardian,* 30 March 2014) < https://www.theguardian.com/culture/2014/mar/30/charlotte-laws-fight-with-internet-revenge-porn-king > accessed 20 February 2022.

[258] ibid.

[259] ibid.

[260] Kashmir Hill, 'How Revenge Porn King Hunter Moore Was Taken Down' (*Forbes,* 21 January 2014) < https://www.forbes.com/sites/kashmirhill/2014/01/24/how-revenge-porn-king-hunter-moore-was-taken-down/?sh=2a03e30948c0 > accessed 20 February 2022.

because of the attention she was bringing to the issue, Charlotte Laws herself became a greater target. Laws received help from the group Anonymous, an international group of hackers, who subsequently crashed Moore's servers to hold Moore 'accountable for his actions'.[261] Charlotte Laws has since campaigned for laws to be enacted that criminalise IBSA. This case shows that the collateral damage of IBSA can extend beyond the primary victim.

Victim	Lessons to be learned about IBSA
'Jane'	IBSA is under-reported and lacks legal intervention and enforcement.
Desire Luzinda	Victim-blaming is a common response to IBSA.
Tyler Clementi	IBSA is not exclusive to images taken, saved and stored. It can also include live footage.
Jennifer Lawrence	Celebrities can be vulnerable and specifically targeted by hackers searching for intimate images.
Holly Jacobs	Victims may never escape the effects of IBSA and may need to resort to changing their name/identity.
'Sarah'	Perpetrators can use IBSA to gain or maintain control and power over their victims. Images taken may be as a result of force and may be used as blackmail.
Audrie Pott	There may be multiple perpetrators carrying out an act of IBSA. Vulnerable people are often used as easy targets.
Kara Jefts	Shaming websites used to label people as having a disease can be used as a platform for IBSA.
Charlotte and Kayla Laws	Damages caused by IBSA can extend beyond the primary victim.

Figure 2 Summary of case examples

1.3.5 Shifting attitudes towards image-based sexual abuse

IBSA was not always viewed as an act worth criminalising, but society's perception of IBSA has evolved over time. The notion that the internet is exempt from social norms

[261] ibid.

leads to a victim-blaming attitude. In the past, the lack of law enforcement responses to online issues owed much to the claim that victims could avoid their problems themselves.[262] Citron explained that some people view the internet as a space with no laws and that people who benefit from its opportunities should also be willing to face its risks. [263] Citron also explained that people believe they have to assume the risk of abuse when using networked tools.[264] As a result, blaming victims is a common response to online abuse.[265] Therefore, it was no surprise that cases of IBSA were initially met with little tolerance or sympathy. This attitude is very similar to how cases of sexual assault were received in the 1970s when, as Lerner and Miller explain, there was a tendency to 'blame victims of misfortunes for their own fates'.[266]

Henry and Powell explain how IBSA was framed as a problem of 'naivete'[267] rather than as a crime. For example, the operator of the 'revenge porn' website 'Texxxan.com' stated: 'when you take a nude photograph of yourself and you send it to this other person, or when you allow someone to take a nude photograph of you, by your very actions you have reduced your expectation of privacy'.[268] Similarly, a journalist urged young people to simply stop 'sharing their naked photos'. She stated that 'this point of view puts me dangerously close to blaming the victim, but we should be telling our daughters and our young women friends that they cannot count on the police, the courts or the legislature to protect them from the consequences of their own poor judgement.'[269] A 2013 qualitative study by Walker, Sanci and Temple-Smith found victim-blaming attitudes in their interviews with 33 young people.[270] Both female and male participants noted that girls who sent sexts are 'viewed as responsible for the potential fallout that proceeds, even though boys may have coerced the girl to send the image'.[271] It is clear that victim-blaming often dominated early societal attitudes towards victims of IBSA –

---

[262] U.S. Department of Justice, *Cyberstalking: A New Challenge for Law Enforcement and Industry* (Washington, DC:GPO 1999).
[263] Danielle Keats Citron, *Hate Crimes in Cyberspace* (1st edn, Harvard University Press 2014) 19.
[264] ibid 79.
[265] ibid 77.
[266] Melvin J. Lerner & Dale T. Miller, 'Just World Research and the Attribution Process: Looking Back and Ahead' (1978) 85 Psychological Bulletin 1030; Sarah Bothamley and Ruth J. Tully, Understanding Revenge Pornography: Public Perceptions of Revenge Pornography and Victim Blaming' (2018) 10 Journal of Aggression Conflict and Peace Research 3.
[267] Nicole Henry and Anastasia Powell, 'Beyond the 'Sext': Technology-Facilitated Sexual Violence and Harassment Against Adult Women' (2015) 48 Australian and New Zealand Journal of Criminology 104.
[268] Callie Millner, 'Public Humiliation over Private Photos' (SF Gate, 10 February 2013) <http://www.sfgate.com/opinion/article/Public-humiliation-over-private-photis-4264155.php.> accessed 4 March 2019.
[269] Susan Reimer, 'Intimate Photos That Would Intimately' *Baltimore Sun* (30 October 2013).
[270] Shelly Walker, Lena Sanci, & Meredith Temple-Smith, 'Sexting: Young Women's and Men's Views on its Nature and Origins' (2013) 52 Journal of Adolescent Health 697.
[271] ibid 699.

most of whom were and are women. The breach of privacy which arises from the non-consensual sharing of intimate images was deemed to be the responsibility of the women who produced, or allowed to be produced, the images in the first place.[272] This view can be linked to Hogg and Vaughan's research that found that 'an individual attributes another's behaviour more to internal than to situational causes'.[273] Furthermore, victims were often considered to be 'over-reacting' to the distribution of their image.[274] Rather than receiving support from society, friends, family or law enforcement, victims were 'scolded' for sharing their intimate images.[275] They were told that they could have 'avoided the abuse had they been more careful'.[276] Not only were victims considered to be over-reacting to the distribution of their intimate image; they were also accused of 'exaggerating the problem' and harm caused.[277] This victim-blaming attitude towards victims of IBSA has been reported as being present within law enforcement. One study shows how 'traditional masculine values, victim-blaming attitudes, and a lack of understanding of gendered violence' contribute to how IBSA has been policed.[278] In many such cases, victims received no guidance or support from the police due to the blaming attitude of the officer.[279]

As education and public discussion increased regarding the harms and risks of the internet, so too did attitudes towards victims of IBSA. Firstly, children were now seen as victims deserving protection. This view was especially evident in much of the research conducted about sexting practices between minors and the need for regulation of these practices.[280] Sexually exploitative material involving minors has always been treated with the utmost seriousness on the major social media sites.[281] However, only in recent times has sexually exploitative material involving adults, particularly IBSA, attracted a similarly strong response.[282] It was not until 2015 that several social media companies,

---

[272] Emma Bond & Katie Tyrrell, 'Understanding Revenge Pornography: A National Survey of Police Officers and Staff in England and Wales' (2021) 36 Journal of Interpersonal Violence 2166.
[273] Michael A. Hogg & Grahem M. Vaughan, *Social Psychology* (4th edn, Pearson Education Limited Essex 2015); Sarah Bothamley and Ruth J. Tully, 'Understanding Revenge Pornography: Public Perceptions of Revenge Pornography and Victim Blaming' (2018) 10 Journal of Aggression Conflict and Peace Research 3.
[274] Danielle Keats Citron, *Hate Crimes in Cyberspace* (1st edn, Harvard University Press 2014)77.
[275] ibid.
[276] ibid.
[277] ibid.
[278] Nicola Henry, Asher Flynn, & Anastasia Powell, 'Policing Image-Based Sexual Abuse: Stakeholder Perspectives' (2018) 19(6) Police Practice and Research 565.
[279] ibid.
[280] Kieran F. McCartan & R. McAlister, 'Mobile Phone Technology and Sexual Abuse' (2012) 21(3) Information & Communications Technology Law 257.
[281] ibid.
[282] Law Reform Commission, Harmful Communications and Digital Safety (LRC 116 — 2016) 3.09.

including Facebook, Twitter and Google, explicitly banned IBSA from their sites amid growing pressure to take action against this type of material. It is evident that victim blaming has become less of an issue. However, it is still present. Its continuing presence was identified, for example, in a 2018 study in which 168 British people participated in an online questionnaire.[283] The questionnaire aimed to establish whether the length of a relationship and the reason for its breakdown influenced victim blaming in IBSA.[284] The study found that victims are not blamed in cases of IBSA and that the length of the victim-perpetrator relationship and the reason for its breakdown did not influence public perceptions of blame.[285] However, it did discover that gender may influence such public perceptions. The study established that men attributed significantly more blame to victims of IBSA than females did, while females rated police intervention as being significantly more important in cases of IBSA than men did.[286] Similarly, in a 2019 Australian study by Henry, Flynn and Powell, a disturbing level of victim-blaming and harm minimisation attitudes were present among respondents.[287] Overall, one in two men and one in three women held attitudes that either minimised the harms or blamed the victims of IBSA. Despite such widely held victim-blaming attitudes among survey respondents, four in five respondents agreed with the statement 'It should be a crime for someone else to share a nude or sexual image of another person without that person's permission'.[288] Therefore, despite victim-blaming still being present in contemporary society, there is certainly an awareness that it should be a crime, and this awareness points to a more victim-centred outlook.

In recent times, significant research has been conducted regarding IBSA abuse as a gendered and minority-focused issue. Some studies have found that, similar to other forms of intimate aggression, women are more commonly the targets of IBSA as compared to men.[289] For example, Cyber Civil Rights Initiative reported that 90% of

[283] Sarah Bothamley and Ruth J. Tully, 'Understanding Revenge Pornography: Public Perceptions of Revenge Pornography and Victim Blaming' (2018) 10 Journal of Aggression Conflict and Peace Research 5.
[284] Sarah Bothamley and Ruth J. Tully, 'Understanding Revenge Pornography: Public Perceptions of Revenge Pornography and Victim Blaming' (2018) 10 Journal of Aggression Conflict and Peace Research 5.
[285] ibid 7.
[286] ibid.
[287] Nicola Henry, Asher Flynn, & Anastasia Powell, 'Responding to 'Revenge Pornography': Prevalence, Nature and Impacts' Report to the Criminology Research Advisory Council Grant: CRG 08/15-16 (March 2019).
[288] ibid.
[289] Marsha Wood, Christine Barter, Nickey Stanley, Nadia Aghtaie, & Cath Larkins, 'Images across Europe: The Sending and Receiving of Sexual Images and Associations with Interpersonal Violence in Young People's Relationships' (2015) 59 Children and Youth Services Review 149.

victims are female and that the majority of perpetrators are men.[290] Furthermore, a study commissioned by the Australian Office of the eSafety Commissioner found that women over the age of 18 were twice as likely as men over this age to have experienced someone sharing nude or sexual images of them without their consent.[291] Qualitative research indicates that a key driver of IBSA is gender inequality, 'including heteronormative masculine power and privilege, as well as the attendant socially constructed norms, values, and attitudes that exist on gender and sexuality'.[292] 'Socially punitive' and 'restrictive norms and expectations' surrounding female sexuality mean that women are often 'punished more harshly for perceived transgressions'.[293] However, research conducted by Lenhart, Ybarra, and Price-Feeney, and Reed, Tolman, and Ward, have found similar victimization rates among both men and women.[294]

In addition to examining the gendered nature of IBSA, several studies have reported differing rates of IBSA victimization according to sexuality, with LGBTIQ (lesbian, gay, bisexual, transgender, intersex, or questioning) participants more likely to report a person having shared a sexual image of them without permission as compared to heterosexual participants.[295] Women of 'colour, religious or ethnic minority women, lesbian, bisexual, transgender or intersex (LBTI) women, women with disabilities, or non-binary individuals who don't conform to traditional gender norms of male and female' often experience online abuse that targets these different identities.[296] This experience is evident in Australia, where IBSA is common among 'Indigenous Australians, LGBTIQ groups, and those with a disability'. [297]

---

[290] Michelle Gonzalez, 'Power in Numbers' **(**Cyber Civil Rights Statistics on Revenge Porn, 3 January 2014) < https://cybercivilrights.org/revenge-porn-infographic/> accessed 14 January 2022.
[291] Office of the eSafety Commissioner, 'National Survey on Image-Based Abuse in Australia' *Report prepared for the Office of the eSafety Commissioner* (Melbourne: RMIT University, 2017)
[292] Nicola Henry, Asher Flynn, & Anastasia Powell 'Policing Image-Based Sexual Abuse: Stakeholder Perspectives' (2018) 19(6) Police Practice and Research 565.
[293] Jessica Ringrose & Emma Renold, 'Slut-Shaming, Girl Power and 'Sexualisation': Thinking through the Politics of the International SlutWalks with Teen Girls' (2012) 24(3) Gender and Education 333.
[294] Amanda Lenhart, Michelle Ybarra, & Myeshia Price-Feeney, *Online Harassment, Digital Abuse and Cyberstalking in America* (Report 11.21.16 Data and Society Research Institute); Anastasia Powell & Nicola Henry, Powell A, & Henry N, 'Technology-Facilitated Sexual Violence Victimization: Results from an Online Survey of Australian Adults' (2019) 17 Journal of Interpersonal Violence 34; Lauren Reed, Richard Tolman, & Monique Ward, 'Snooping and Sexting: Digital Media as a Context for Dating Aggression and Abuse Among College Students' (2016) 22(13) Violence Against Women 1556.
[295] Amanda Lenhart, Michelle Ybarra, & Myeshia Price-Feeney, *Online Harassment, Digital Abuse and Cyberstalking in America* (Report 11.21.16 Data and Society Research Institute); Gisela Priebe, & Carl Göran Svedin, 'Online or Off-line Victimization and Psychological Wellbeing: A comparison of Sexual-Minority and heterosexual youth' (2012) 21(10) European Child & Adolescent Psychiatry 569.
[296] Emma Bond and Katie Tyrrell, 'Understanding Revenge Pornography: A National Survey of Police Officers and Staff in England and Wales' (2021) 36 Journal of Interpersonal Violence 2166.
[297] Nicola Henry, Anastasia Powell & Asher Flynn, *Not just 'Revenge Pornography': Australians' Experiences of Image-Based Abuse: A Summary Report* (Melbourne: RMIT University 2017).

1.4 Mediums which facilitate image-based sexual abuse

1.4.1 How the internet assists image-based sexual abuse

The internet has brought enormously positive benefits to society,[298] although it has also caused harm. As discussed, IBSA is not a new phenomenon, but its 'prevalence, reach, and impact' have increased with the advent and development of the internet.[299] People can access private intimate images quickly and easily. Internet service providers allow people access to the internet and search engines connect them to the IBSA material. Content providers such as social media sites and dedicated websites that host IBSA provide perpetrators with a platform and viewers the opportunity to engage with the material. Such intimate images are thereby exposed to billions of viewers, while often allowing perpetrators a degree of anonymity.[300]

The internet often provides perpetrators with a feeling of disconnection from the harm they cause.[301] Individuals feel that their online behaviour is set apart from their 'real world' behaviours. Therefore, although an individual may not disclose a private, intimate image in person, while online they feel safer and disconnected from their action due to their physical distance and their feeling that their actions do not translate into the real world in any real or moral/criminal sense. They care less or feel that they will not be caught. The perception of anonymity (frequently perceived rather than actual) in digital communications prompts individuals to act in a manner they would not in the offline world.[302] It may also increase the anxiety the victim experiences, since the pool of potential perpetrators may be far wider than in the offline setting, leaving the victim unable to identify who originally posted their intimate image.[303]

The instant nature of digital communications may increase the harm caused to victims of IBSA as it leads to a greater volume of and more frequent communications than would occur in an offline context and this increases the number of viewers of the image. The potential to reach large, global audiences and the overwhelming exposure that may result can magnify the harm. The easy accessibility of the internet, where an individual can

[298] Mary Ann Franks, *Drafting an Effective "Revenge Porn " Law: A Guide for Legislators* (Cyber Civil Rights Initiative, 2 November 2015).
[299] ibid.
[300] Dylan Love, 'It Will Be Hard to Stop the Rise of Revenge Porn' *Business Insider* (8 February 2013)
[301] Law Reform Commission, Harmful Communications and Digital Safety (LRC 116 — 2016).
[302] ibid.
[303] ibid.

upload an image instantly, also creates a challenge as once the perpetrator decides to post an image there is often no screening system and it may be very difficult to have the image taken down. As stated by Penny, the internet 'never forgets. And that permanent digital record, a blessing when it summons a moment we want to recall with the click of a mouse, can be a weapon in more sinister hands when it preserves one we would like to forget'.[304] The permanence of the material combined with the searchability of the web means that damaging intimate images can survive long after their initial posting and associated harm and can be used to revictimise the target each time the image is accessed.[305]

The global nature of the internet leads to jurisdictional issues that further complicate the effective application of IBSA laws.[306] Some jurisdictions have targeted legislation, while others do not. It is very difficult to take effective action to have IBSA material removed from the internet when it is hosted on servers in a different jurisdiction to the victim, particularly where the other jurisdiction does not have laws against IBSA. Furthermore, the age of consent differs from jurisdiction to jurisdiction, creating ambiguity as to what constitutes IBSA and what amounts to indecent images of children.

1.4.2 Platforms for image-based sexual abuse

Most cases of IBSA feature a combination of three participants in the online communication - the party that posts the content, the party that accesses the content, and the party which enables the first two to communicate – the intermediary. 'Internet intermediaries' is an umbrella term for individuals and organisations which facilitate the use of the internet.[307] They have been described as follows:

> Internet intermediaries bring together or facilitate transactions between third parties on the Internet. They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties.[308]

O'Doherty considers the term internet intermediaries to broadly comprise the following, separate categories of providers:

- Internet service providers ('ISPs'), which provide services for accessing and using the internet. These can be sub-divided further into those organisations which simply connect users to the internet ('internet access providers'), and

[304] Jonathon Penny, 'Deleting Revenge Porn' (*Policy Options Politiques*, 1 November 2013) < https://policyoptions.irpp.org/fr/magazines/vive-montreal-libre/penney/ > accessed 20 February 2022.
[305] Law Reform Commission, Harmful Communications and Digital Safety (LRC 116 — 2016).
[306] ibid.
[307] Michael O'Doherty, *Internet Law* (1st edn, Bloomsbury Professional 2020) [1.66].
[308] OECD, 'The Economic and Social Role of Internet Intermediaries' (April 2010) <https://www.oecd.org/sti/ieconomy/44949023.pdf > accessed 20 February 2022.

those which provide electronic mail ('email') hosting, website hosting and domain name registration. Many ISPs perform more than one of these functions.
- Internet search engines and portals.
- E-commerce intermediaries, where these platforms do not take title to the goods being sold, ie online marketplaces and auction sites such as Amazon and eBay.
- Internet payment systems.
- Participative networking platforms,[309] which include internet publishing and broadcasting platforms that do not themselves create or own the content being published or broadcast, to include social media platforms, blogging platforms, video sharing websites, online gaming sites and instant messaging platforms.[310]

Social media platforms and 'revenge pornography' websites are of particular relevance in the context of IBSA as they facilitate the perpetration of these behaviours and as a result will be discussed in more detail below.

Social Media Platforms

Social media sites are an extremely significant element of modern internet usage and have many valuable functions. Social media sites have been defined as: 'web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system.'[311] Therefore, the key feature of social media sites is a public or semi-public profile through which users connect with other users.[312] Social media sites are premised on the concept of sharing content with others. Sharing content has become common practice, with large sections of society comfortable with habitually sharing personal information with a wide social network.[313] Stroud and Henson point out that social media sites allow users to instantly share content without much reflection about the 'wisdom or value of such communications'.[314] Mark Zuckerberg, the founder of Facebook, stated that 'people have really gotten comfortable not only sharing more information and different kinds, but more

[309] 'Participate networking platforms' are referred to as 'online content sharing service providers' in Article 17 of the Digital Copyright Directive 2019, see chapter on Intellectual Property, para 7.78.
[310] Michael O'Doherty, *Internet Law* (1st edn, Bloomsbury Professional 2020) [1.68].
[311] Danah M. Boyd & Nicole B. Ellison, 'Social Network Sites: Definition, History, and Scholarship' (2008) 13 Journal of Computers Media and Communication 210, 211.
[312] Law Reform Commission, Harmful Communications and Digital Safety (LRC 116 — 2016).
[313] ibid.
[314] Scott Stroud and Jonathan Henson, 'Social Media, Online Sharing and the Ethical Complexity of Consent in Revenge Porn' In A. Close (ed.), *Online Consumer Behavior: The Dark Side of Social Media* (United States: Routledge Press 2017) 13-32.

openly and with more people. That social norm is just something that has evolved over time'.[315]

The enormous popularity of social media sites and the extent to which they have become embedded in 21st century society has led to the creation both of new crimes and a new space for committing existing offences. According to Franks, one in eight social media users have been targets of IBSA.[316] The Law Reform Commission's consultation workshop with young people discovered that social media sites are the most popular avenue for disseminating intimate images without consent in Ireland.[317] While these sites provide an easy and quick avenue to share content, the removal of such content can be very difficult. Social media sites appear to be reluctant to remove material unless it is obviously illegal in nature, such as child pornography. Under non-statutory, self-regulated policies, individuals can report harmful content to social media sites and request that it be removed. However, not all material is treated in the same way and procedures vary among companies.[318] In a survey of 4122 women aged between 115-45 conducted by the Office of the eSafety Commissioner in 2017 found that the main social media sites used to disseminate IBSA material were Facebook and Snapchat, which are discussed in greater detail below.[319] Other significant social media sites include WhatsApp, Instagram, Twitter, YouTube, Tik Tok, LinkedIn, and Discord. In 2013, every minute YouTube users uploaded 100 hours of new videos, Instagram users shared over 41,000 new photos, and Twitter users tweeted over 347,000 times.[320] These figures have significantly increased. In 2017, Instagram users posting over 46,740 photos every minute and Twitter users tweeting over 456,000 times every minute.[321] As of February 2020, more than 500 hours of video were uploaded to YouTube every minute. [322]

---

[315] Bobbie Johnston, 'Privacy No Longer a Social Norm, Says Facebook Founder' (*The Guardian*,11 January 2010) < https://www.theguardian.com/technology/2010/jan/11/facebook-privacy > accessed 20 February 2022.

[316] Mary Ann Franks, 'Drafting an Effective 'Revenge Porn' Law: A Guide for Legislators' (*Cyber Civil Rights Initiative,* 22 September 2016) 3 <https://www.cybercivilrights.org/wp-content/uploads/2016/09/Guide-for-Legislators-9.16.pdf> accessed 24 August 2022.

[317] Law Reform Commission, Harmful Communications and Digital Safety (LRC 116 — 2016) Appendix B.

[318] ibid.

[319] Office of the eSafety Commissioner, 'National Survey on Image-Based Abuse in Australia' *Report prepared for the Office of the eSafety Commissioner* (Melbourne: RMIT University, 2017).

[320] Danielle Keats Citron, *Hate Crimes in Cyberspace* (1st edn, Harvard University Press 2014).

[321] Bernard Mar, 'How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read' <https://www.bernardmarr.com/default.asp?contentID=1438 >accessed 20 February 2022.

[322] Statista, 'Hours of video uploaded to YouTube every minute as of February 2020' < https://www.statista.com/statistics/259477/hours-of-video-uploaded-to-youtube-every-minute/ > accessed 20 February 2022.

Facebook

Adding to the sixty million photos uploaded to Instagram every day, in 2013 Facebook users were uploading over three hundred million photos to Facebook.[323] Facebook alone has more than 2.89 billion users and is currently the world's most popular social media site, with a net worth of over $86 billion.[324] In 2018 it was reported that every minute on Facebook, more than 500,000 comments are posted, almost 300,000 statuses are updated, and more than 130,000 photos are uploaded.[325] With hundreds of millions of photos uploaded each day, the potential for IBSA heightens. According to a 2016 Ipsos MRBI Poll on Social Networking, 64% of people in Ireland have Facebook accounts.[326] Moreover, 72% of them use Facebook daily. Facebook allows users to set up a profile in their own name, share information, post pictures and videos, message other users and comment on content shared by them.[327]

SnapChat

SnapChat allows users to send photos and videos that are only briefly viewable and so the only way the recipient can continue to view them is by taking a screenshot for further viewing later. According to SnapChat, 'the data is completely deleted and could not be recalled even if law enforcement came looking for it'.[328] However, this statement is somewhat misleading as further investigation into the company's privacy policy reveals that although SnapChat attempts to delete all image data, it cannot guarantee that the content is deleted in every case and so messages are sent at the user's risk.[329] Furthermore, there is still a chance that the recipient may take a screenshot of the image (a photo of the image seen on the screen of a phone) that saves the received photo to their photo album.[330] Even though the application will notify the sender that the screenshot has been taken,

[323] Casey Martines, 'An Argument for Sates to Out Law Revenge Porn and for Congress to Amend 4 U.S.C and 230: How our Current Laws Do Little to Protect Victims' (2014) 14 Pittsburgh Journal of Law and Policy 235-238.
[324] Statista, 'Number of daily active Facebook users worldwide as of 4th quarter 2021' < https://www.statista.com/statistics/346167/facebook-global-dau/#:~:text=With%20roughly%202.89%20billion%20monthly,most%20popular%20social%20network%20worldwide > accessed 20 February 2022.
[325] Barry O'Sullivan, 'Social Media Giants Must be Excluded from Online Safety Watchdog Role' *Irish Times* (Dublin, 21 July 2018).
[326] Ipsos MRBI, 'Social Networking Quarterly' (April 2016) <http://ipsosmrbi.com/wpcontent/uploads/2016/05/SN_Apr16.png . > accessed 4 March 2019.
[327] Corey Omer, 'Intermediary Liability for Harmful Speech: Lessons from Abroad' (2014) 28(1) Harvard Journal of Law & Technology 289-324.
[328] Lindsey Bever, 'Fighting Back against Revenge Porn' *Washington Post* (Washington, 28 April 2014).
[329] Danielle Citron & Mary Franks, 'Criminalizing Revenge Porn' (2014) 49 Wake Forest Law Review 34.
[330] Aysegul Harika, 'Banning Revenge Pornography: Florida' (2014) 39 Nova Law Review 65.

once the photo is copied the sender has little control over what the recipient will do with the image.[331] This has the potential to lull a user into a false sense of security before sharing an intimate image they would not want shared beyond that context.

'Revenge pornography' websites

As noted above, acts of IBSA have contributed to an entirely new genre of pornography, with at least 3,000 pornography websites hosting a 'revenge pornography' genre.[332] Consequently, by 2010 'revenge pornography' websites were set up specifically to receive and show IBSA material. According to Citron, in 2014 there were 40 sites that trafficked IBSA material.[333] Purveyors of IBSA material manage websites that solicit sexually explicit photos without the subjects' consent.[334] Hunter Moore's website, 'IsAnyoneUp.com', best exemplified the practice. A variety of people - ranging from jilted ex-lovers or hackers to bored browsers - submit these photos.[335]

Hunter Moore founded and managed the now-defunct website, 'IsAnyoneUp.com', achieving infamy as a self-professed 'professional life ruiner'.[336] His extremely popular 'revenge pornography' website received 30 million page views a month and featured thousands of explicit pictures.[337] Moore stated that he received 10,000 submissions of images in three months and that his site generated $8,000 to $13,000 in advertising revenue per month.[338] The website encouraged jilted lovers in possession of intimate photos to send these photos to Moore.[339] Not only did the site solicit for naked photos, but the submission form asked for the subject of the image's name, a link to their Facebook or Twitter page, and other personal information.[340] This information ensured

[331] ibid.
[332] Clara McGlynn & Erika Rackley, 'More than Revenge Porn: Image-Based Sexual Abuse and the Reform of Irish Law' (2017) 14 Irish Probation Journal 38.
[333] Danielle Keats Citron, *Hate Crimes in Cyberspace* (1st edn, Harvard University Press 2014) 51.
[334] Alex Jacobs, 'Fighting Back Against Revenge Pornography: A Legislative Solution' (2016) 12(1) Northwerstern Journal of Law and Social Policy.
[335] ibid.
[336] Emily Zemler, 'Naked & Famous: How a Risque New Website Pushes Boundaries and Buttons' (14 February 2011) <http://www.altpress.com/features/entry/naked-famous-how_a-risque-new website-pushes boundaries and buttons.> accessed 4 March 2019.
[337] Memphis Barker, 'Revenge Porn Is No Longer a Niche Activity Which Victimises Only Celebrities-The Law Must Intervene' *Independent* (19 May 2013).
[338] Kashmir Hill, 'Revenge Porn with a Facebook Twist' (Forbes, 6 July 2011) < https://www.forbes.com/sites/kashmirhill/2011/07/06/revenge-porn-with-a-facebook-twist/?sh=1abc8a2e1d2e > accessed 20 February 2022.
[339] Alex Jacobs, 'Fighting Back Against Revenge Pornography: A Legislative Solution' (2016) 12(1) Northwerstern Journal of Law and Social Policy.
[340] Kashmir Hill, ''Revenge porn with a Facebook twist' (Forbes, 6 July 2011) < https://www.forbes.com/sites/kashmirhill/2011/07/06/revenge-porn-with-a-facebook-twist/?sh=1abc8a2e1d2e > accessed 20 February 2022.

that the image would appear prominently in a Google search of those key identifiers.[341] Though the website only existed for 16 months, it had a significantly negative effect on the lives of Moore's victims, who included celebrities, musicians, school teachers and politicians.[342] Moore shut down IsAnyoneUp.com in April 2012 due to legal pressures concerning child pornography.[343] In October 2013, Moore was indicted for accessing a protected computer without authorisation to obtain information for private financial gain.[344]

Another 'revenge pornography' website, operated by Kevin Christopher Bollaert, was ugotposted.com. This website facilitated the posting of more than 10,000 explicit images of individuals without their consent.[345] Bollaert also required that the victim be identified by name, age, and other information. Bollaert was arrested on 31 counts of conspiracy, identity theft and extortion in California for his role in creating the website.[346] Bollaert took it a step further than Moore by charging victims from $250 to $350 to remove images of them through another website, changemyreputation.com. [347]

MyEx.com was another 'revenge pornography' website, founded in 2013 and owned by Web Solutions B.V. Netherlands. It provided people with a platform to anonymously upload and share images and videos of ex-partners and other people they knew.[348] Unlike other 'revenge pornography' websites, MyEx.com allowed both posters and viewers to engage with the material they encountered through comments and specific search facilities.[349]

1.4.3 The concept of 'sexting' and 'selfies'

Sexting

[341] Alex Jacobs, 'Fighting Back Against Revenge Pornography: A Legislative Solution' (2016) 12(1) Northwestern Journal of Law and Social Policy.
[342] Alex Morris, 'Hunter Moore: The most hated man on the internet' (Rolling Stone, 11 October 2012) < https://www.rollingstone.com/culture/culture-news/hunter-moore-the-most-hated-man-on-the-internet-184668/ > accessed 20 February 2022.
[343] ibid.
[344] Jessica Roy, 'Revenge-Porn King Hunter Moore Indicted on Federal Charges' *Time* (23 January 2014).
[345] Aysegul Harika, 'Banning Revenge Pornography: Florida' (2014) Nova Law Review 65.
[346] The Associated Press, 'California: Man Is Charged in 'Revenge Porn' Case' *New York Times* (New York, 10 December 2013).
[347] Don Thompson, 'Court Date Set for Kevin Bollaert in Revenge Porn Website Case' *Huffington Post* (12 December 2013).
[348]Matthew Hall and Jeff Hearn, *Revenge Pornography Gender, Sexualities and Motivations* (Routledge: New York 2018).
[349] ibid.

Rapid developments in technology, and the opportunities new technological innovations provide for communication, have led to the emergence of 'sexting'.[350] The term 'sexting' first appeared in the tabloid media in 2005 after allegations emerged that Australian cricketer, Shane Warne, had sent sexually explicit text messages to three women in three continents.[351] Subsequently, 'sexting' became a subject of much public, media and scholarly debate. Sexting can be defined as the practice of sending or posting sexually explicit text messages and images, both still and video, including nude or semi-nude photographs, via a device or over the internet.[352] Typically, a person takes a digital photo of himself or herself and sends it via a mobile phone as a text message.[353] These devices permit the images to be easily shared with the entire world due to changes in camera capabilities on mobile phones that enable images to be taken and then uploaded onto an array of other platforms with relative ease.[354] The now widespread practise of sexting facilitates IBSA. Minors and young adults are exploring their sexuality through sexting 'in a more dangerous way by leaving permanent traces of the fruits of their exploration'.[355] Despite the risks of this, sexting may also have benefits for some users. For example, it allows partners to remain intimate even while separated in space or time[356] and may help people to overcome inhibitions and feel better able to express attraction and sexual feelings.[357] Recent surveys show that sending and posting explicit images and videos starts at a young age and becomes more frequent as teenagers become young adults.[358] In a survey conducted in 2012 in over 600 high schools in America, 20% of the students had sent a sext from their phone and 40% had received a sext. More than one quarter had forwarded a sext to others that they had received.[359] A 2019 study by Henry,

---

[350] Nicola Henry and Anastasia Powell, 'Beyond the 'Sext': Technology Facilitated Sexual Violence and Harassment Against Adult Women' (2015) 48(1) Australian & New Zealand Journal of Criminology 104.
[351] James, O. 'He's Clean Bowled by a Sick Need for Pleasure' *Daily Telegraph* (2 July 2005).
[352] *Miller v. Skumanick,* 605 F. Supp. 2d 634 (M.D. Pa. 2009) (No. 3:09cv540).
[353] Ausegul Harika, 'Banning Revenge Pornography: Florida' (2014) 39 Nova Law Review 65
[354] Australian Parliament Joint Select Committee on Cyber-safety, *High-wire act: Cyber-safety and the young, interim report* (Canberra, Australia: Commonwealth of Australia 2011 — 146); Victorian Parliamentary Law Reform Committee, *Inquiry into sexting: Report of the Law Reform Committee Inquiry into Sexting (*Parliamentary Paper No.230, 2011Melbourne, VIC: State Government of Victoria).
[355] Elizabeth Ryan, 'Sexting: How the State can prevent a moment of indiscretion from leading to a lifetime of unintended consequences for minors and young adults' (2010) 96 Iowa Law Review 357.
[356] Jessica Leshnoff, Sexting Not Just for Kids, (AARP, June 2011) < http://www.aarp.org/relationships/love-sex/info-11-2009/sexting_not_just_for_kids.html > accessed 20 February 2022. (describing a relationship coach whose client was 'a wife who enjoys sexting her husband while he's traveling on business, telling (and showing) him what he's missing at home').
[357]Yvonne K. Fulbright, 'Scintillating Sexting' (Psychology Today, 14 September 2012) <https://www.psychologytoday.com/ie/blog/mate-relate-and-communicate/201209/scintillating-sexting> accessed 20 February 2022
[358] Nicole Poltash, 'Snapchat and Sexting: A Snapshot of Baring your Bare Essentials' (2014) 19(4) Richmond Journal of Law and Technology 1.
[359] ibid.

Flynn and Powell revealed that nearly half of its 4,274 respondents had taken an intimate image of themselves and engaged in sexting.[360] According to the Cyber Civil Rights Initiative, 80% of IBSA victims had sent their intimate image with consent while sexting. This type of cyber-activity has been assisted by readily available and inexpensive smart technology and the emergence of image-sharing apps such as Instagram, Snapchat and WhatsApp. As the use of these communications increases, so too do the numbers of people who fall victim to IBSA.

Selfies

A selfie is defined as a self-shot photograph, taken at arms-length or in front of a mirror, and one that is both a 'photographic object that initiates the transmission of human feeling in the form of a relationship', and a 'practice or gesture that can send different messages to different recipients'.[361] Although self-portraits existed in the past, 'selfies' have emerged and developed due to the smartphone and the proliferation of social networking.[362] Visual communication has become a common use of the mobile phone.[363] New functionalities of smartphones, such as the front-facing camera and the possibility to share content online, have turned 'selfies' into a mainstream cultural practice.[364] The sending of intimate selfies is an expression of intimacy in relationships in the digital age and has fast become a 'normative part of flirting and intimate exchanges'.[365] This development in the way relationships are conducted has also led to an increase in the harms that can be caused when a relationship breaks down. 80% of IBSA images are 'selfies.[366] Although the majority of naked or intimate 'selfies' are generated within a

[360] Nicola Henry, Asher Flynn, & Anastasia Powell, 'Responding to 'Revenge Pornography': Prevalence, Nature and Impacts' Report to the Criminology Research Advisory Council Grant: CRG 08/15-16 (March 2019) 32.
[361] Theresa Senft & Nancy Baym. 'What Does the Selfie Say? Investigating a Global Phenomenon' (2015) 9 International Journal of Communication1588.
[362] Ji Won Kim & T. Makana Chock, 'Personality Traits and Psychological Motivation Predicting Selfie Posting Behaviours on Social Networking Sites' (2017) 34 Telematics and Informatics 560.
[363] Lasén, A., 'Autofotos. Subjetividades y Medios Sociales' [Selfies: Subjectivities and Social Media]. In García-Canclini N, & Cruces F, (eds.) *Jóvenes, Culturas Urbanas y Redes Digitales. Prácticas Emergentes en las Artes, el Campo Editorial y la Música [Young People, Urban Cultures and Digital Networks. Emerging Practices in Arts, Editorial Field and Music]* (Madrid: Ariel 2012); Barbara Scifo, 'The Domestication of Camera-Phone and MMS Communication. Early Experiences of Young Italians' In K. Nyìri (Ed.) *The Global and the Local in Mobile Communication* (Wien: Passagen Verlag 2005).
[364] Giovanna Mascheroni, Jane Vincent & Estefania Jinenez, 'Girls are Addicted to Likes so they Post Semi-Naked Selfies': Peer Mediation, Normativity and the Construction of Identity Online' (2015) 9(1) *Cyberpsychology: Journal of Psychosocial Research on Cyberspace.*
[365] Edgar Gómez Cruz & Christina Miguel, 'I'm Doing This Right Now and It's for You: The Role of Images in Sexual Ambient Intimacy' in M. Berry, and M. Schleser (eds) *Mobile Media Making in an Age of Smartphones* (New York: Palgrave Macmillan 2014).
[366] Amanda Levendowski A, 'Using Copyright to Combat Revenge Porn' (2014) N.Y.U Journal of Intellectual Property and Entertainment Law 422.

romantic relationship,[367] other such 'selfies' may be generated to explore identity[368] or as a tool for 'self-improvement and self-knowledge'.[369] As a result, an individual may store a selfie image on a device that is later hacked, leading to the dissemination of the image without their consent. The development of 'selfie' culture has increased the creation of intimate images which, in turn, increases the potential for the creation of further victims in the future.

1.5 The application of existing laws to image-based sexual abuse

As IBSA — facilitated by the development of internet and technology — escalated into a global phenomenon, attempts were made to address the harm caused through the use of existing civil and criminal laws. The traditional laws and approaches have limitations that have been attempted to be addressed in some jurisdictions by the passage of targeted criminal laws and through the development of regulatory systems targeting specific 'online harms' including IBSA. These measures are discussed later in this thesis, but it is first necessary to briefly address how existing civil and criminal approaches could be applied to IBSA. To date, there is a wealth of academic literature on the range of applicable civil and criminal laws addressing cases of IBSA. Much of the literature focuses on developments in the United States,[370] although notable analyses have considered the situation other jurisdictions such as Australia,[371] Japan[372] and Scotland.[373] Examples of existing laws used against IBSA include privacy, data protection, copyright, defamation, and harassment.

---

[367] Anatasia Powell & Nicola Henry, 'Blurred Lines? Resonding to 'Sexting' and Gender-based Violence amoung Young People' (2014) 39(2) Children Australia 119.
[368] Amparo Lasén, *Understanding Mobile Phone Users and Usage* (Newbury: Vodafone Group R&D 2005).
[369] Jill Walker Rettberg, *Seeing Ourselves through Technology: How We Use Selfies, Blogs and Wearable Devices to See and Shape Ourselves* (Palgrave Macmillan 2014).
[370] Danielle Citron & Mary Ann Franks, 'Criminalizing Revenge Porn' (2014) 49(2) Wake Forest Law Review 345; Danielle Keats Citron, *Hate Crimes in Cyberspace* (1st edn, Harvard University Press 2014).
[371] Nicola Henry & Anastasia Powell, 'Beyond the 'Sext': Technology-Facilitated Sexual Violence and Harassment Against Adult Women' (2015) 48(1)Australian and New Zealand Journal Criminology 104; Nicolas Suzor, Bryony Seignior, & Jennifer Singleton, 'Non-Consensual Porn and the Responsibilities of Online Intermediaries' (2017) 40(3) Melbourne University Law Review 1057; Dan Svantesson, 'Sexting and the Law: How Australia Regulates Electronic Communication of Non-Professional Sexual Content' (2010) 22(2) Bond Law Review 41; Michael Salter & Thomas Crofts, 'Responding to Revenge Porn: Challenging Online Legal Impunity' in Comella, L. and Tarrant, S. (eds.) *New Views on Pornography: Sexuality, Politics and the Law* (Praeger Publisher: Westport 2015) 233–253.
[372] Shigenori Matsui, 'The Criminalization of Revenge Porn in Japan' (2015) 24(2) Washington International Law Journal 289.
[373] Rachel Hill, 'Cyber-Misogyny: Should 'Revenge Porn' be regulated in Scotland, and if so, How?' (2015) 12(2) SCRIPTed.

1.5.1 Privacy

While the need for privacy has been recognised for thousands of years [374] it has also been criticised in more recent times as a 'moribund right'.[375] Within the Irish context, privacy has been described as '[a] complex of rights, varying in nature, purpose and range, each necessarily a facet of the citizen's core of individuality within the constitutional order'.[376] Privacy is an issue that arises in different factual contexts and has clear relevance in the context of IBSA.[377] As mentioned earlier, the right to privacy is protected by several sources of law. The right to privacy is not absolute and may give way to competing rights such as freedom of expression. The vast majority of online cases which entail breaches of privacy involve the distribution of a victim's personal data, including imagery of the victim.[378] However, the use of privacy in cases of IBSA does have limitations. In the US context, Pitcher criticises privacy actions in two main ways: 'impotence' and 'constitutional conflict with other rights'.[379] Impotence, according to Diane Zimmerman, 'contends . . . that despite the ever-increasing number of claims under the Warren-Brandeis theory, plaintiffs rarely win'.[380] The lack of success of privacy claims can be regarded as a practical limitation to their use, at least in the US context. Some question whether litigation under privacy laws is worth the 'further embarrassment and public disclosure of private facts'.[381] Such litigation for breach of privacy may bring greater attention to the victim of IBSA through their intimate images since their name may be made public, enabling people to find the private material online. Another challenge privacy actions face is where the legal standard requires the plaintiff's 'reasonable expectation of privacy' to have been violated. It may be argued that when a person shares an intimate image with someone else, they have surrendered their reasonable expectation

[374] Jan Holvast, 'History of Privacy' in Vashek Matyas and others (eds), *The Future of Identity in the Information Society* (Springer 2009) 15.
[375] Rónán Kennedy and Maria Helen Murphy, *Information and Communications Technology Law in Ireland* (1st edn, Clarus Press 2017) 133.
[376] *Norris v Attorney General* [1984] IR 36 at 71, 80 (per Henchy J.)
[377] Tom Gotsis, *Revenge Pornography,Privacy and the Law* (NSW Parliamentary Research Service — e-brief Issue 7/2015).
[378] Submissions of Digital Rights Ireland to *Issues Paper on Cyber-crime Affecting Personal Safety, Privacy and Reputation Including Cyber-bullying* (2015).
[379] Justin Pitcher, 'The State of the States: The Continuing Struggle to Criminalize Revenge Porn' (2016) 2015 Brigham Young University Law Review 1435.
[380] Diane L. Zimmerman, 'Requiem for a Heavy weight: A Farewell to Warren and Brandeis's Privacy Tort' (1983) 68 Cornell Law Review 291, 293.
[381] Justin Pitcher, 'The State of the States: The Continuing Struggle to Criminalize Revenge Porn' (2016) 2015 Brigham Young University Law Review 1435.

of privacy.[382] Larkin points out that sharing an image with a trusted confidante 'should not be equated to consent for it to be exposed to the public at large'.[383] In Ireland, due to the guarantee of privacy in the Constitution, a victim may seek an injunction or damages for its violation. Injunctions, particularly interim injunctions, have been regarded as a vital remedy for victims claiming a threatened breach of personal privacy.[384] Interim injunctions are regarded as the most effective as, once an individual's privacy has been breached, the ability to fully remedy the harm is removed, and so prevention of the posting in the first place is important.[385]

1.5.2 Data Protection

Data protection law provides a framework for the use of personal data that also protects the 'fundamental rights and freedoms of natural persons and in particular their right to the protection of their personal data'.[386] While the right to protection of personal data and the right to respect for private life are 'distinct legal rights' within the EU legal order,[387] there is a clear connection between data protection and privacy.[388] The General Data Protection Regulation (GDPR) provides the general legislative framework for data protection in the EU. An intimate image of an identifiable natural person clearly constitutes 'personal data' and thus it receives protection under the GDPR.[389] A person is often identifiable by their image alone, but perpetrators of IBSA also often upload intimate images with attached information such as their names, addresses, contact numbers or places of employment. Indeed, an intimate image is likely to qualify as special category data and thus be subject to additional protections.[390] Article 4(2) of the GDPR defines processing as 'any operation or set of operations which is performed on personal data or on sets of personal

---

[382] *Laskey and Ors v The United Kingdom* (1997) 24 EHRR 39 – dealt with privacy in an S&M context; See *A.H. v State*, 949 So. 2d 234, 237 (Fla. Dist. Ct. App. 2007) for an early IBSA court decision espousing this view.

[383] Paul J. Larkin, 'Revenge Porn, State Law, Free Speech' (2014) 48 Loyola of Los Angeles Law Review 24.

[384] Helen Fenwick & Gavin Phillipson, *Media Freedom under the Human Rights Act* (Oxford University Press, 2006) 807; Eric Barendt, *Freedom of Speech* (2nd edn, Oxford University Press 2006) 137.

[385] Gavin Phillipson, 'Max Mosley goes to Strasbourg: Article 8, Claimant Notification and Interim Injunctions' (2009) 1 Journal of Media Law 73, 74; *Mosley v News Group Newspapers Limited* [2008] EWHC 1777 (QB) (24 July 2008) [230]- [231].

[386] The General Data Protection Regulation 2016/679, art 1(2).

[387] Charter of Fundamental Rights of the European Union 2000/C 364/01, art 7 & art 8; Rónán Kennedy and Maria Helen Murphy, *Information and Communications Technology Law in Ireland* (Clarus Press 2017) [5-06].

[388] Nadezhda Purtova, 'Private Law Solutions in European Data Protection: Relationship to Privacy, and Wavier of Data Protection Rights' (2010) 28(2) Netherlands Quarterly of Human Rights 179.

[389] The General Data Protection Regulation 2016/679, art 4(1).

[390] Data Protection Act 2018, s 2 & The General Data Protection Regulation 2016/679, art 9 regard 'personal data concerning an individual's sex life or sexual orientation' as an area which needs special protection.

data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.[391]

The GDPR does not apply to 'a natural person in the course of a purely personal or household activity'.[392] This is known as the 'household exemption'.[393] This exemption may cause some confusion for victims of IBSA as many cases occur during personal relationships whereby the parties engage in the 'purely personal' activity of sexting, generally within their own home. However, when individuals post personal data on a public website about another person without an adequate legal basis, the exemption will not apply because making information available for all to see is not regarded as a purely personal or recreational purpose and the user will assume the full responsibility of a data controller.[394] The Article 29 Data Protection Working Party has stated that, where a user has 'a high number of third party contacts some of whom he may not actually know' the household exemption may not apply and the user would be considered a data controller.[395] Therefore, if an individual posts personal information about another person on a publicly available website or social networking page that is accessible to a large number of people, the individual may be considered a data controller. Consequently, cases of IBSA will often not fall under this exception.

It is clear that IBSA falls within the scope of the GDPR. Data protection laws offer victims a number of remedies for IBSA. Data protection law provides for a complaints system where an individual can report a data controller for unlawful processing of their personal data to the Data Protection Commission. Moreover, Article 79 of the GDPR provides the right to an effective judicial remedy against a controller or processor. It means that victims

[391] The General Data Protection Regulation 2016/679, art 4(2).
[392] ibid art 2(2)(c).
[393] Data Protection Working Party Opinion 5/2009 on online social networking 01189/09/EN WP 163 (June 2009), art 29.
[394] See *Bodil Lindqvist v Åklagarkammaren i Jönköping* (C-101/01) [2004] ECR I 12971, paragraph 47, in which the EU Court of Justice stated in connection with the "household exemption" in Article 3.2 of Directive 95/46/EC: "That exception [the household exemption] must therefore be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people." This case concerned a woman who was charged with breaching Swedish Data Protection legislation for publishing on her website personal data on a number of people she worked with. A number of questions were referred to the EU Court of Justice including whether the woman was a data controller; Law Reform Commission, Harmful Communications and Digital Safety (LRC 116 — 2016) para 2.107.
[395] Data Protection Working Party Opinion 5/2009 on online social networking 01189/09/EN WP 163 (June 2009), art 29.

of IBSA have a right to apply for damages or an injunction to prevent the processing of their data or to remove unlawfully processed data. Article 82 of the GDPR provides victims with the right to compensation. Article 82(1) states that 'Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered'.[396] Victims of IBSA can suffer great mental anguish, so the provision of a remedy specific to this harm is beneficial.[397] The main aim of victims of IBSA tends to be the removal of the material from the internet and the Article 17 GDPR 'right to erasure' would appear to respond to that aim. Article 17 GDPR provides that data subjects have the right to the erasure of personal data concerning them in a number of situations. Section 92(4) of the 2018 Act requires a data controller or processor to 'erase the data as soon as may be and, in any event, no later than one month after the date' upon which a request is made.[398] The right to erasure may be an option in some cases of IBSA, although the time period of one month can be seen as being too long. This delay can be of concern because by the time a right of erasure has been upheld, the material in question may have been more broadly disseminated. It has also been argued that this right 'strongly encourages internet intermediaries to delete challenged content, even if the challenge is legally groundless'[399] because, while there are no consequences for over-removing content, intermediaries risk very large fines for not fulfilling right to be forgotten requests.[400]

1.5.3 Copyright

Copyright law may also be considered as a potential action to take against IBSA. The purpose of copyright law is to protect 'authors' creative expression', 'incentivise the creation of new works', and 'serve the public interest' by making those works available for use and enjoyment.[401] Copyright law is concerned with the 'flow of creative property'.[402] When a person creates a work, ownership of that work belongs to the creator.

---

[396] The General Data Protection Regulation 2016/679, art 82(1).
[397] Eoin O'Dell, 'Compensation for Breach of the General Data Protection Regulation' (2017) 40(1) Dublin University Law Journal 97.
[398] Data Protection Act 2018, s 92(4).
[399] Daphne Keller, "Final Draft of Europe's 'Right to be Forgotten' Law" (The Center for Internet and Society, Stanford Law School, 17 December 2015) < http://cyberlaw.stanford.edu/blog/2015/12/final-draft-europes-right-be-forgotten-law > accessed 20 February 2022.
[400] Law Reform Commission, Harmful Communications and Digital Safety (LRC 116 — 2016) para 3.41.
[401] Twentieth Century Music Corp. v. Aiken, 422 U.S. (1975).
[402] Jonathan Zittrain, What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication, (2000) 52 Standford Law Review1201, 1203.

The core issue when copyright law is violated is non-consensual appropriation and use. In IBSA cases involving 'selfies', copyright law could be used to claim ownership of the images, thereby prohibiting others from posting them on the internet without their consent.[403] Reproducing or displaying images without the author's permission infringes upon the author's copyright.[404] Images created as the result of work by both the photographer and the subject of the photograph can create joint ownership.

Copyright can be a powerful tool for victims of IBSA who have taken the images themselves.[405] The Copyright and Related Rights Act 2000 provides immediate protection to the author of the copyrighted work. The author of an image is the person who recorded the image.[406] This protection gives the author exclusive rights to reproduce, publish, and communicate the work.[407] Accordingly, a perpetrator infringes copyright law when he/she distributes an image that he/she did not take. For a victim of IBSA to have rights over their intimate image, the victim must be the author of the image. Levendowski had described copyright law as providing 'a uniform method for revenge porn victims to remove their images, target websites that refuse to comply with takedown notices and, in some cases, receive monetary damages'.[408] Although 80% of intimate images are 'selfies' - meaning that the photographer and the image subject are the same - copyright law would typically not be useful for the remaining portion of victims.[409] While copyright can be directly applied to a significant number of IBSA cases, it is not without limitations. Similar to data protection, copyright ignores one of the key 'moral evils' of IBSA.[410] It does not recognise the harm associated with the breach of trust and 'lacks the expressive effect of a societal condemnation' of the behaviour of disseminating intimate images without the subject's consent.[411] Copyright fails to consider the nature of the harms of 'violation of dignity and sexual autonomy'.[412] Moreover, the litigious use of copyright

[403] Amanda Levendowski, 'Using Copyright to Combat Revenge Porn' (2014) N.Y.U Journal of Intellectual Property and Entertainment Law 422.
[404] ibid.
[405] Amanda Levendowski, 'Using Copyright to Combat Revenge Porn' (2014) New York University Journal of Intellectual Property and Entertainment Law 422; Jessica Lake, '"Overexposed": Legal Responses to the Unauthorised Publication of Private Photos' (2016) 3 Australian Media, Technology and Communications Law Bulletin 8, 9.
[406] Copyright and Related Offences Act 2000, s 21(h).
[407] ibid.
[408] Amanda Levendowski, 'Using Copyright to Combat Revenge Porn' (2014) N.Y.U Journal of Intellectual Property and Entertainment Law 422, 426.
[409] ibid.
[410] Ari Ezra Waldman, 'A Breach of Trust: Fighting Nonconsensual Pornography' (2017) 102 Iowa Law Review 709.
[411] ibid.
[412] Anastasia Powell and Nicola Henry, *Sexual violence in a digital age* (Palgrave Macmillan 2017) 216.

can cause further harm since the victim is named during the litigation, which can lead to further viewings of the image online.[413] Remedies under copyright include injunctions and damages.

1.5.4 Defamation

While not immediately obvious, defamation laws may in some instances be of relevance in the IBSA context. Section 6(2) of the Defamation Act 2009 provides that 'the tort of defamation consists of the publication, by any means, of a defamatory statement concerning a person to one or more than one person (other than the first-mentioned person)'.[414] A 'defamatory statement' means a statement that tends to injure a person's reputation in the eyes of a reasonable member of society. Such a statement can be made orally or in writing and includes visual images, sounds, gestures and any other method of signifying meaning. The basis of a defamatory action is injury to one's reputation. Therefore, it must be proved that the statement was communicated to someone other than the person defamed. In some jurisdictions, the plaintiff must show the harm caused as a result of the defamatory statement. In Ireland, the plaintiff only has to prove that the defamation occurred and does not need to show the harm caused as a result of the defamatory statement. That said, there are many legal defences available to perpetrators who carry out acts of defamation. In Ireland these include truth, absolute privilege, qualified privilege, honest opinion, fair and reasonable publication on a matter of public interest, consent, and innocent publication.[415] There is no dispute that the dissemination of an intimate image or video can be damaging to a person's reputation.[416] The issue with applying defamation to IBSA cases is that often the shared image will be an accurate representation of an event. Defamatory issues may arise if the intimate image is posted with a caption containing defamatory material, for example an image may be posted alongside a name, phone number and advertisement for sex work as seen in the case *X v Twitter*.[417] However these situations are limited by the facts. Digital Rights Ireland has

[413] Julia M. Sorensen, 'Forgive and Regret: Analysis and Proposed Changes to Connecticut's Revenge Porn Statute' (2017) 35 Quinnipiac Law Review 559, 592.
[414] Defamation Act 2009, s 6(2).
[415] See for example Defamation Act 2009, s16-27.
[416] Danielle Citron & Mary Ann Franks, 'Criminalizing Revenge Porn' (2014) 49 Wake Forest Law Review 34.
[417] In the case of *X v Twitter*, the Irish High Court granted an injunction directing Twitter to remove from its platform 'grossly defamatory and offensive sexually related pictures and tweets' about a teacher. A fake Twitter profile had been created purporting to be the profile of the plaintiff teacher in order to 'post sexually explicit pictures of her, as well as identifying the town where she lived and worked.' The judge granted the injunction against Twitter, and directed that, although the hearing would be conducted in public, neither her identity nor her profile should be identified by the media. See X v Twitter [2011] EWHC 3454; Ray

pointed out that the courts have long taken the view that crude and vulgar abuse is not necessarily defamatory.[418] Within the Irish context there are six remedies available to victims under Sections 28-34 of the Defamation Act 2009. These are: summary disposal, declaratory order, correction order, lodgement, orders restraining publication, and damages which will be assessed below. Under Section 33 of the Act, a court may, upon application of a plaintiff, make an order prohibiting the publication of the defamatory statement (injunction), or further publication of the statement in question, if in its opinion the statement is defamatory, and the defendant has no defence to the action that is likely to succeed.[419] Section 31 of the Act provides for the provision of damages. The section considers aggravated factors when awarding compensation, which may be beneficial in cases of IBSA. Such factors include the 'nature and gravity' of the disseminated image, which would consider the content of the image, the extent to which it was 'circulated' (audience reach), and the 'means of publication'.[420]

1.5.5 Harassment

Harassment is 'words, conduct, or other actions, generally repeated or persistent and directed at a specific person, that tend to annoy or cause harassment, alarm, or distress to another person'.[421] A core element in cases of harassment is a course of conduct or persistent behaviour. Acts of harassment are deemed to exist when a person's right to a peaceful and private life is violated, and not just when acts give rise to fear of violence.[422] Within the Irish context, harassment is governed by the Non-Fatal Offences against the Person Act 1997 as amended by the Harassment, Harmful Communications and Related Offences Act 2020. Section 10, defines harassment as occurring when 'Any person who, without lawful authority or reasonable excuse, by any means including by use of the telephone, harasses another by persistently following, watching, pestering, besetting or communicating with or about him or her'.[423] A person harasses another where they 'intentionally or recklessly, seriously interferes with the other's peace and privacy or

Managh, 'Twitter ordered to remove "defamatory" profile of Irish teacher' I*rish Times* (Dublin, 31 December 2013); Pauline Walley, 'In Memory Amore: Revenge, Sex and Cyberspace' (2015) 20(2) The Bar Review 33.

[417] *X v Twitter* [2011] EWHC 3454.

[418] Submissions of Digital Rights Ireland to *Issues Paper on Cyber-crime Affecting Personal Safety, Privacy and Reputation Including Cyber-bullying* (2015).

[419] Defamation Act 2009, s 33.

[420] ibid s 31.

[421] Graham Gooch and Michael Williams, *A Dictionary of Law Enforcement* (2nd edn, Oxford University Press 2015).

[422] Law Reform Commission, *Harmful Communications and Digital Safety* (LRC 116 — 2016) 9.77.

[423] ibid.

causes alarm, distress or harm to the other' and 'his or her acts are such that a reasonable person would realise that the acts would seriously interfere with the other's peace and privacy or cause alarm, distress or harm to the other'.[424] Although harassment under Section 10 of the 1997 Act may apply to online offences, it does not adequately protect victims of IBSA. Indirect harassment is particularly pertinent in the context of IBSA. Prior to 2020, Section 10 only outlawed harassment entailing direct communication with the victim but failed to consider communication about the victim. Section 10 previously required harassment to include a person 'persistently following, watching, pestering, besetting or communicating with him or her' while also interfering with the other's person's peace and privacy causing alarm, distress or harm.[425] However, the definition did not explicitly provide for indirect communication. It did not include a distinction between speech or images about another person and communications made to that person.[426] However the Harassment, Harmful Communications and Related Offences Act 2020 amended Section 10 to include:

> (a) in subsection (1), the substitution of "communicating with or about him or her" for "communicating with him or her",
> (b) in subsection (3), the substitution of "communicate by any means with or about the other person" for "communicate by any means with the other person"[427]

This was a significant amendment as the majority of cases of IBSA occur when the perpetrator posts an intimate image online for the attention of the victim's friends, family, employer or just the general public. The perpetrator seldom sends the image directly to the victim alone. However, IBSA generally occurs by means of a single post that subsequently spreads when other viewers share the image and thus the law on harassment will often not be applicable to cases of IBSA. The penalties under Section 10 consist of a fine and/or imprisonment, which can be for a term not exceeding 12 months on summary conviction and up to ten years on conviction on indictment.[428] As an alternative, or in addition, to any other penalty, the court may issue an order restraining the defendant from communicating with the victim or requiring the defendant to remain a certain distance from the victim's place of residence or employment for a period the court specifies.[429]

[424] Non – Fatal Offences Against the Persons Act 1997, s 10.
[425] ibid.
[426] ibid.
[427] Harassment, Harmful Communications and Related Offences Act 2020.
[428] Non - Fatal Offences Against the Person Act 1997, s 10(6).
[429] ibid s 10(3).

Overall, while there is an array of existing laws applicable to IBSA, the use of non-targeted pre-existing laws to tackle acts of IBSA are 'piecemeal'[430], 'inadequate'[431], and contain 'glaring gaps and inconsistencies'.[432] Furthermore, the first priority of the majority of victims has been reported to be the removal of their intimate image and the second to be the prosecution of the perpetrator.[433] The provision of remedies and penalties such as damages and fines fail to achieve the desired outcome of content removal and as a result there is a need to look to alternative remedies. Notwithstanding this, access to remedies through traditional civil claims is challenging. Civil litigation is very expensive, and many victims cannot afford to hire legal representation.[434] If a victim can afford to proceed with litigation, the process can be extremely difficult and lengthy.[435] In the meantime, intimate images can be continuously circulated, increasing the harm to the victim.

1.6 A brief overview of the development of internet regulation

As set out in sections 1.2.2 and 1.2.3, prior to 1990, the vast majority of internet use entailed a one-way flow of communication whereby the internet was primarily made up of static content posted on websites without any input or interaction on the part of the readers or viewers. In the late 1990s and early 2000s the internet evolved, and former consumers of the internet became users generating their own content. Users of the internet were now able to interact via a variety of online platforms. While this development has been set out above, it is also important to understand how the law has reacted.

The importance of the internet has long been recognised and has been acknowledged by courts including the Court of Justice of the European Union (CJEU), the European Court

[430] Elle Hunt, 'Victoria Leads Way in Piecemeal Approach to Outlawing Revenge Porn', (*The Guardian*, 5 September 2016) < https://www.theguardian.com/australianews/2016/sep/05/victoria-leads-way-in-piecemeal-approach-to-outlawing-revenge-porn > accessed 20 February 2022.
[431] Miles Godfrey, 'Revenge Porn Spreading like Wildfire', (*The Australian*, 22 November 2013) < http://www.theaustralian.com.au/news/latest-news/revenge-pornspreading-like-wildfire/story-fn3dxiwe-1226766034486 > accessed 20 February 2022.
[432] AAP, 'NSW Govt to Consider "Revenge Porn" Laws', (The Australian, 3 March 2016), < http://www.theaustralian.com.au/news/latest-news/let-revenge-porn-victims-sue-nswreport/news-story/e620808a31d2578c773627c9c3451257 > accessed 20 February 2022.
[433] Nicola Henry, Asher Flynn, & Anastasia Powell, 'Policing image-based sexual abuse: stakeholder perspectives' (2018) 19(6) Police Practice and Research 565
[434] Julia M. Sorensen, 'Forgive and Regret: Analysis and Proposed Changes to Connecticut's Revenge Porn Statute' (2017) 35 Quinnipiac Law Review 559, 592.
[435] Alyse Dickson, 'Revenge Porn: A Victim Focused Response' (2016) 2 UniSA Student Law Review 42-69.

of Human Rights (ECtHR) and the US Supreme Court. These sources highlight the internet as a vital resource in the functioning of the modern economy and in the exercise of fundamental rights.[436] Historically, Governments sought to foster the commercial development of the internet by enabling the online industry to develop relatively free from regulation.

Since the emergence of the internet, the liability of intermediaries has been considered a problematic issue.[437] Providers of intermediary services quickly became concerned about the 'potential negative consequences of liability on growth and innovation', 'their lack of effective legal or actual control over the content posted on the internet', and 'the inequity of imposing liability upon a mere intermediary'.[438] As a result the internet industry launched a plea for immunity for third party content.[439] In response, policy makers around the world developed limited liability regimes or safe harbours as will be discussed in section 1.5.1. However, it has become apparent over time that the powerful position the internet industry has taken in our lives requires a level of regulation which ensures that those using its services are protected from harmful, illegal or dangerous postings.[440] As a result, the emphasis has shifted from the protection of the nascent commercial internet by protecting intermediaries, to the promotion of self-regulation and voluntary regulation, to the increased imposition of regulatory responsibilities on intermediaries as will be outlined in section 1.5.2.

1.6.1 Safe harbours developed to protect intermediaries

In the late 1990's and early 2000's an important aim of many governments was to encourage the growth of intermediaries in the hope that this would facilitate economic growth. Ensuring a safe market for content owners to do business appeared a secondary

[436] Council of Europe, Recommendation CM/Rec (2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet; *Ahmet Yildirim v Turkey* (App No 3111/10) 18 December 2012 para 54 'The Internet has now become one of the principal means by which individuals exercise their right to freedom of expression and information, providing as it does essential tools for participation in activities and discussions concerning political issues and issues of general interest'; *Times Newspapers Ltd (Nos. 1 and 2) v United Kingdom* [2009] (App Nos 3002/03 and 23676/03), para 27. 'In light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information generally.'

[437] Aleksandra Kuczerawy,' Intermediary liability & freedom of expression: Recent developments in the EU notice & action initiative' (2015) 31 Computer Law & Security Review 46-56.

[438] OECD, Directorate for Science, Technology and Industry, Committee for Information, Computer and Communication Policy, The Role of Internet Intermediaries In Advancing Public Policy Objectives, Forging partnerships for advancing public policy objectives for the Internet economy, Part II (2011) 6, 11.

[439] ibid.

[440] Lynelle Briggs, *Report of the Statutory Review of the Enhancing Online Safety Act 2015 and the Review of Schedules 5 and 7 to the Broadcasting Services Act 1992 (Online Content Scheme)* October 2018.

consideration against the important economic gains intermediaries promised to offer.[441] As such, leveraging the internet as a source of economic growth by providing adequate incentives for internet businesses to prosper and flourish very much influenced policy formulation and regulation.[442] The aim of legislation was to create an 'enabling mechanism'[443] to support the growth of intermediaries.

Section 230 of the Communications Decency Act 1996 (CDA) is an early example of one of these laws which provides protection to intermediaries in the US context. Section 230 of the CDA protects internet providers from liability for content posted by others. Section 230 of the CDA provides that an internet service provider (ISP) that simply serves as a digital bulletin board is not liable for content created, developed, or posted on or through the ISP's site, unless the ISP somehow curated the content.[444] Section 230(c) of the CDA details the 'Protection for "Good Samaritan" blocking and screening of offensive material'.[445] This section states that '[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.'[446] Congress concluded that without such protections, freedom of speech would be negatively affected.[447] The CDA establishes that a victim can sue the person who is directly responsible for causing harm online. It gives platforms the right, but not the responsibility, to remove content as they see fit.[448] Furthermore, it ensures that platforms do not have to monitor content that users post in advance and will not be held liable just because they provide the services that third parties use to harm others. In the context of IBSA, this regulatory scheme places ISPs that host IBSA (including social media sites and internet search engines) beyond the scope of liability for any damages or any equitable remedies.[449] Therefore, ISPs that host IBSA generally operate with immunity under the CDA.

In the European Union, the E-Commerce Directive 2000/31 (ECD) sets out the framework for electronic commerce by, among other things, regulating certain aspects of

[441] Roya Ghafel, 'From enabling to levelling: the need to change the policy rationale of the intermediary liability regime' (2016) 25 Information & Communications Technology Law 129.
[442] ibid.
[443] ibid.
[444] Communications Decency Act 1996, 47 U.S.C. § 230.
[445] ibid § 230(c).
[446] ibid.
[447] Jessica A. Magaldi, Jonathan S. Sales, & John Paul, 'Revenge Porn: The Name Doesn't Do Nonconsensual Pornography Justice and the Remedies Don't Offer the Victims Enough Justice' (2020) 98 Oregon Law Review 197, 209.
[448] Tarleton Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (1st edn, New Haven CT: Yale University Press 2018) 36.
[449] Layla Goldnick, 'Coddling the Internet: How the CDA Exacerbates the Proliferation of Revenge Porn and Prevents a Meaningful Remedy for its Victims' (2015) 21 Cardozo Journal or Law & Gender 583.

online intermediaries' liability, including the liability of online intermediaries for third-party content. Section 4 of the ECD regulates the liability of intermediary services providers. Articles 12–14 under the ECD shield intermediaries from monetary liability for unlawful activities by users of the provider's services. The Directive addresses three types of intermediaries: 'mere conduit', 'cache' and 'host'. Article 12 governs 'mere conduits' and provides that ISPs are not liable for the information transmitted, on condition that they do not initiate the transmission, do not select the receiver of the transmission, and do not select or modify the information contained in the transmission. Article 13 governs 'caching' and establishes that ISPs are not liable for the automatic, intermediate and temporary storage of that information, if the ISPs cannot modify that information and if they expeditiously remove or disable access to that information, once they learn that it has been removed from the network, or that access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement. Article 14 of the ECD governs 'hosting' and provides a defence against liability, to online hosts, provided certain conditions are met. In particular, hosts of third party content are not liable, as long as: (a) they do not have actual knowledge of the illegality of that content and, as regards claims for f, awareness of facts or circumstances from which the illegality is apparent; or (b) upon obtaining such knowledge, they act expeditiously to remove or to disable access to the content.[450] Under Article 15 of the ECD, intermediaries have no general obligation to monitor information they transmit or store. They also cannot be obliged to actively look for facts or circumstances indicating illegal activity.[451]

Both the CDA and the ECD consist of two basic principles which demonstrates the safe harbour approach to internet regulation. Both approaches do not hold intermediaries responsible for third-party content hosted on their platform provided they do not modify that content and are not aware of its illegal character. Furthermore, both hold no general obligation for intermediaries to monitor content on their platform.

1.6.2 The shift against safe harbours - responsibilities imposed on intermediaries

As opportunities for sharing ideas and information on the internet multiply, debate on the role and responsibilities of intermediaries has increased around the world.[452] Following

[450] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce) [2000] OJ L 178/1.
[451] E-Commerce Directive 2000/31/EC, art 15.
[452] Lisl Brunner, 'The Liability of an Online Intermediary for Third Party Content The Watchdog Becomes the Monitor: Intermediary Liability after Delfi v Estonia' (2016) 16 Human Rights Law Review 163-174;

countless public relations scandals, large-scale privacy breaches, and growing concerns about polarization and misinformation, there has been an increasing demand for 'external governance.'[453] A gradual rethinking of intermediary responsibility and liability appears to be occurring.

Four important cases which highlight a shift away from the strict protection of the established safe harbours are the Court of Justice of the European Union cases of *Google France v Louis Vuitton,*[454] *L'Oréal v eBay,*[455] and *Google Spain SL v Gonzalez,*[456] and the ECtHR case of *Delfi v Estonia*.[457] In *Google France v Louis Vuitton* and *L'Oréal v eBay,* the CJEU offered some insights on how to interpret Article 14 of the ECD so to clarify the boundaries of ISPs' liability. It established that, the ISP is exempted from any form of liability if it is ascertained that its conduct was merely technical, automatic and passive. However, the Court clarified that an ISP which has not played an active role cannot, however, enjoy the safe harbour set forth by Article 14, if it has been informed of facts or circumstances on the basis of which a diligent operator should have recognized the illegal conduct and has not promptly acted to prevent its recurrence by removing infringing materials or by disabling access to subjects who have entered such materials online.[458] In *Google Spain SL v Gonzalez,* the CJEU ruled that search engines had an obligation to remove links to personal information on the internet that were inaccurate, inadequate, irrelevant or excessive.[459] This ruling was made through an application of the Data Protection Act read in light of the Charter of Fundamental Rights of the European Union. In 2015, the ECtHR held that it was not a violation of the ECHR where an online news portal was held liable in domestic law for comments posted to its site by third parties even though the portal lacked knowledge of the unlawful nature of the comments and promptly removed them when requested to do so.[460] While this ruling was by the ECtHR and was

---

Dimitroff Kallen, 'Mark Zuckerberg, Joe Manchin, and ISIS: What Facebook's International Terrorism Lawsuits Can Teach Us About the Future of Section 230 Reform' (2021) 100 Texas Law Review; Camille Bachrach, 'The case for a safe harbor provision of CDA 230 that allows for injunctive relief for victims of fake profiles' (2020) 72 Federal Communications Law Journal 147; Jeff Hermes, 'Section 230 as Gatekeeper: When Is an Intermediary Liability Case Against a Digital Platform Ripe for Early Dismissal?' (2017) 43 American Bar Association 34; Natalia Homchick, 'Reaching Through the "Ghost Doxer:" An Argument for Imposing Secondary Liability on Online Intermediaries' (2019) 76 Washington & Lee Law Review 1307.

[453] Robert Gorwa, 'What is platform governance?' 22 Information, Communication & Society 854.

[454] Case C-236/08 *Google France v Louis Vuitton Malletier SA and others* (2010) ECLI:EU:C:2010:159.

[455] Case C-324/09 *L'Oréal SA and others v eBay International AG and others* (2011) ECLI:EU:C:2011:474.

[456] *Google Spain SL v Gonzalez,* No. C-131/12 (Court of Justice of the European Union May 13, 2014).

[457] *Delfi v Estonia* Application No 64569/09, ECtHR, 16 June 2015.

[458] Case C-236/08 *Google France v Louis Vuitton Malletier SA and others* (2010) ECLI:EU:C:2010:159; Case C-324/09 *L'Oréal SA and others v eBay International AG and others* (2011) ECLI:EU:C:2011:474.

[459] *Google Spain SL v Gonzalez,* No. C-131/12 (Court of Justice of the European Union May 13, 2014).

[460] *Delfi v Estonia* Application No 64569/09, ECtHR, 16 June 2015.

limited to a consideration of whether the ECHR had been infringed and not EU law, this could be perceived as a further strike against the concept of intermediary liability.

While case law demonstrates that intermediary liability exemptions are not absolute, Suzor states that new laws being introduced around the world are also imposing greater responsibilities on intermediaries to help combat issues such as hate speech and online disinformation.[461] For example, the German Network Enforcement (NetzDG) law removes liability protections for content violating German law, mandating that platforms remove 'evidently unlawful' material in less than 24 hours following a complaint or face significant fines of up to €50 million.

> Many different jurisdictions are steadily expanding existing laws that govern privacy, defamation, consumer protection, and many other topics to apply to intermediaries of all types, from content hosts to search engines to infrastructure companies like internet service providers and even online payment processors.[462]

While the ECD regime of safe harbour remains,[463] the context in which it applies has been impacted by the Digital Single Market Directive,[464] amendments to the Audiovisual Media Services Directive,[465] guidance on the enforcement of intellectual property rights,[466] and recommendations for combating harmful online content.[467] While the ECD exemptions continue to be a key element of the European system for intermediary liability, these initiatives place different 'layers of obligations'[468] on online platforms.

The Digital Single Market Strategy aimed to evolve the EU from 28 national markets to 'a connected digital single market' by 'bringing down barriers to unlock online

---

[461] Nicolas Suzor, *Lawless: The Secret Rules that Govern our Digital Lives* (Cambridge University Press 2019).

[462] ibid.

[463] European Commission, 'Online platforms and the Digital Single Market — Opportunities and Challenges for Europe' Communication 288/2 (25 May 2016) 9.

[464] European Commission, 'Proposal for a Directive on copyright in the Digital Single Market' Communication 593 final (14 September 2016).

[465] European Commission, 'Proposal for a Directive amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audio-visual media services in view of changing market realities' Communication 287 final (25 May 2016).

[466] European Commission, 'Guidance on certain aspects of Directive 2004/48/EC of the European Parliament and of the Council on the enforcement of intellectual property rights' Communication 708 final (29 November 2017).

[467] European Commission, 'Tackling Illegal Content Online - Towards an enhanced responsibility of online platforms' Communication 555 final (28 September 2017); European Commission, 'Commission Recommendation on measures to effectively tackle illegal content online' Communication 1177 final (1 March 2018).

[468] Maria Lilla` Montagnani, Safe harbours in deep waters: a new emerging liability regime for Internet intermediaries in the Digital Single Market (2018) 26 International Journal of Law and IT 294.

opportunities'.[469] The Digital Single Market Strategy covers a variety of policy topics including the role of intermediaries. In particular, the Commission considered 'whether to require intermediaries to exercise greater responsibility and due diligence in the way they manage their networks and systems'—a duty of care'.[470] In response to the Digital Single Market Strategy the Commission launched a comprehensive assessment of the role of online platforms including how best to tackle illegal content on the internet, copyright infringing content, child abuse content and racist and xenophobic speech being among the listed examples.[471] Following this assessment, the Commission published a communication entitled 'Online platforms and digital single market, opportunities and challenges for Europe',[472] which highlighted the rising importance of intermediaries and the need to have them operate in a balanced regulatory framework.[473] It also highlighted the importance of ensuring online platforms behave responsibly. The Commission stated that the existing intermediary liability regime would be maintained, however a 'problem-driven approach' to regulation would be implemented which included changes to the Audiovisual Media Services Directive (AVMSD) and copyright law.[23] Both of these amendments demonstrate a shift away from pure immunity of intermediaries however, in the context of this thesis, the amendments to the AVMSD is of more relevance and will be briefly outlined further to highlight this shift.

In May 2018, the EU Commission as part of the Digital Single Market Strategy proposed a revision of the AVMSD 2010 [474] with a particular focus on the issue of combating hate speech and dissemination of harmful content to minors. As a result, a new set of obligation for AVMS operators were introduced. In October 2018, the European Parliament approved the revised AVMSD, which was followed by approval from the Council in November 2018.[475] Member States were given 21 months to implement the amendments within their national regimes.

---

[469] European Commission, 'A Digital Single Market Strategy for Europe' Communication 192 final (6 May 2015).

[470] ibid.

[471] European Commission, *Public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy* (24 September 2015).

[472] European Commission, 'Online platforms and the Digital Single Market — Opportunities and Challenges for Europe' Communication 288/2 (25 May 2016) 9.

[473] ibid.

[474] Directive of European Parliament and the Council 2010 13/EU of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) [2010] OJ L 95/1.

[475] European Parliament, Legislative resolution on the proposal for a directive of the European Parliament and of the Council amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media

One of the main changes to the AVMSD is that its terms were broadened to cover 'video-sharing-platforms'.[476] Video-sharing platforms are defined as commercial services addressed to the public, where the principal purpose of the service (or an essential functionality of it) is devoted to providing programs and user-generated videos to the general public. Although the Commission states that these platforms do not have editorial control over the user content they host, they are expected to prevent adult content, such as pornography or advertisements for alcohol, from being made readily available to children.[477] They are also expected to prevent access to content which is hateful to minority ethnic groups, as well as content which seeks to incite violence.[478] Such measures are to be adopted without prejudice to Article 12 to 15 of the ECD.

The AVMSD lists some examples of appropriate measures for platforms to achieve these new obligations. These include flagging mechanisms enabling users to report illegal content to the hosting platform and requiring platforms to then remove the reported material within a specific timeframe, the length of which is determined by the illegal nature of the content.[479] Other measures include age verification systems, content rating systems, parental control systems, media literacy measures and tools, and raising users' awareness of those measures and tools, and easy-to-use and effective procedures for the handling and resolution of users' complaints to the video-sharing platform provider in relation to the implementation of the measures. Under the amended Article 28b, these measures 'shall not lead to any ex-ante control measures or upload filtering of content which do not comply with Article 15 of Directive 2000/31/EC'. [480]

As evident above, in recent years the European Commission has become increasingly dissatisfied with the liability framework for internet intermediaries. A large part of this dissatisfaction stems from the fact that hosting platforms are under no obligation to actively seek out and remove illegal user content from their services.[481] They must only remove this content if they have received explicit notice of its existence.[482] Since 2017

services in view of changing market realities', Communication (2016)0287 – C8-0193/2016 – 2016/0151(COD) (2 October 2018).

[476] European Parliament and Council, 'Proposal for amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities Communication (2016) 287 final, Recital 7a. Recital 3b.

[477] Audiovisual Media Services Directive 2010, art 28a(1)(a).

[478] ibid art 28a(1)(b).

[479] ibid.

[480] Audiovisual Media Services Directive 2010, art 28b.

[481] Michael Russ, 'Problematically Proactive: a Summary of Recent Legal Developments In the Field of Internet Intermediary Liability' (2018) 69 Northern Ireland Legal Quarterly 563.

[482] ibid.

the Commission has sought to encourage hosts to actively remove illegal content from their services instead of waiting to receive knowledge of it through a notice-and-takedown order.[483] This active removal of content as demonstrated above through the example of the AVMSD is to be achieved through platforms undertaking voluntary 'proactive measures'. These voluntary proactive measures are to be consistent with the Article 15 no monitoring obligations.

The Digital Services Act (DSA) and the Digital Markets Act (DMA) are the two most recent legislative initiatives, proposed by the European Commission, with the aim of upgrading rules governing digital services in the EU. The principal goal of the DMA is the establishment of a level playing field to foster innovation, growth, and competitiveness, both in the European Single Market and globally. However, of particular relevance in the context of this thesis is the DSA. The DSA's principal goal is the creation of a safer digital space within which the fundamental rights of all users of digital services are protected. The DSA intends to build on the rules set out in the e-commerce Directive. The DSA intends to cover digital service providers that act as intermediaries offering either a mere conduit service, a caching service, or a hosting service.[484] As a result, providers such as internet service providers, domain name registrars, social media networks, messaging services, cloud services, app stores, and online platforms would all fall under the scope of the DSA. Obligations include measures to counter illegal content[485] online, such as a mechanism for users to flag such content, effective safeguards for users to challenge platforms' content moderation decisions, and obligations for very large online platforms to prevent the misuse of their systems. In the context of intermediary liability, the DSA places diligence obligations regarding illegal content onto various categories of service providers. Article 10 lays down obligations applicable to all providers of intermediary services, in particular: the obligation to establish a single point of contact to facilitate direct communication with Member States' authorities. Article 13 requires

[483] Commission, 'Tackling Illegal Content Online' Communication (2017) 555 final; Commission Recommendation C/2018/1177 of 1 March 2018 on measures to effectively tackle illegal content online [2017] OJ L63/50.

[484] Digital Services Act, article 2(f) states: 'intermediary service' means one of the following services: –a 'mere conduit' service that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network; –a 'caching' service that consists of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request; –a 'hosting' service that consists of the storage of information provided by, and at the request of, a recipient of the service.

[485] Digital Services Act, article 2(g) states: 'illegal content' means any information, which, in itself or by its reference to an activity, including the sale of products or provision of services is not in compliance with Union law or the law of a Member State, irrespective of the precise subject matter or nature of that law.

all service providers to adhere to transparency reporting obligations in relation to the removal and the disabling of information considered to be illegal content or contrary to the providers' terms and conditions. Article 14 requires hosting service providers to put in place mechanisms to allow third parties to notify the presence of alleged illegal content. Furthermore, all online platforms must provide an internal complaint-handling system in respect of decisions taken in relation to alleged illegal content or information incompatible with their terms and conditions.[486] The DSA also obliges online platforms to engage with certified out-of-court dispute settlement bodies to resolve any dispute with users of their services.[487] Furthermore, online platforms are also obliged to publish reports on their activities relating to the removal and the disabling of information considered to be illegal content or contrary to their terms and conditions.[488] In the context of very large online platforms,[489] Article 26 and Article 27 requires these platforms to conduct risk assessments on the systemic risks brought about by or relating to the functioning and use of their services and to take reasonable and effective measures aimed at mitigating those risks. While the strengthening of intermediary responsibility is evident within the DSA, there was concerns that the Commission did not specifically address either the 'gendered nature of online abuse, nor the extent of non-consensual pornography available online'.[490] In response, the European Parliament strengthened the DSA in relation to user generated pornography, resulting in a new clause, Article 24b which states:

> Where an online platform is primarily used for the dissemination of user generated pornographic content, the platform shall take the necessary technical and organisational
> measures to ensure:
> (a) that users who disseminate content have verified themselves through a double opt-in email and cell phone registration;
> (b) professional human content moderation, trained to identify image-based sexual abuse, including content having a high probability of being illegal;
> (c) the accessibility of a qualified notification procedure in the form that additionally to the mechanism referred to in Article 14 individuals may notify the platform with the claim that image material depicting them or purporting to be depicting them is being disseminated without their consent and supply the platform with prima facie evidence of their physical identity; content notified through this procedure is to be suspended without undue delay.[491]

[486] Digital Services Act, article 17.
[487] ibid article 18.
[488] ibid article 23.
[489] Digital Services Act, article 25 defines very large platforms as platforms reaching at least 45 million users in the EU representing 10% of the population.
[490] Lorna Woods & Clare McGlynn, 'Pornography platforms, the EU Digital Services Act and Image-Based Sexual Abuse' (*Media@LSE blog*, 26 January 2022) < https://blogs.lse.ac.uk/medialse/2022/01/26/pornography-platforms-the-eu-digital-services-act-and-image-based-sexual-abuse/ > accessed 25 February 2022.
[491] Digital Services Act, article 24b.

Article 24b provides clear recognition of the prevalence and harms of IBSA. In particular, this article seeks to reduce, and ultimately prevent, many cases of IBSA by requiring extra checks in the process of uploading and disseminating material which makes the process more time -consuming and also allows for the identification of the uploader. While traditional avenues of redress such as reporting to the police remain important in providing redress for many victims once the abuse has taken place, Article 24b and indeed Articles 10-27 of the DSA have the potential to reduce the incidence of IBSA occurring.

Overall, while there has been a shift from absolute immunity, intermediaries still maintain a level of protection and many responsibilities imposed under various emerging laws can be shaped and implemented at the discretion of the intermediary. Issues arise when voluntary measures fail to respond to harm caused to victims of online acts such as IBSA or when intermediaries ignore their regulatory obligations. Furthermore, there are also concerns that voluntary solutions may be less transparent and fail to provide sufficient due process safeguards.[492] These failings in the context of IBSA are evident and are addressed in Chapter 2 when explaining why Australia developed the Office of the eSafety Commissioner and in Chapter 4 and Chapter 5 when outlining the current Irish situation with regard to IBSA and the need for an enforcement response.

1.7 Image-based sexual abuse and conflicting rights

1.7.1 Privacy v free expression

As discussed earlier, a core issue present in cases of IBSA is the breach of the victim's right to sexual privacy. Privacy is generally viewed as a 'multi-faceted' right that is complex, varying in nature, purpose, and range, and is the 'core of individuality within the constitutional order'.[493] In spite of receiving protection in multiple national, regional, and international human rights documents, privacy is not an absolute right and can be restricted by the constitutional rights and interests of others.

There is a risk that the over-regulation of content hosted by intermediaries could cause a chilling effect on freedom of expression as it could result in intermediaries erring

[492] Nicolas Suzor, Bryony Seignior & Jennifer singleton, 'Non-consensual porn and the responsibilities of online intermediaries' (2017) 40 Melbourne University Law Review 1057; Nicola Henry and Asher Flynn, 'Image-Based Sexual Abuse: Online Distribution Channels and Illicit Communities of Support' (2019) 25 Violence Against Women 1932; Nicolas Suzor, *Lawless: the secret rules that govern our digital lives* (Cambridge University Press 2019).
[493] *Norris v Attorney General* [1984] IR 36.

on the side of caution and removing legitimate content.[494] The right to freedom of expression is considered 'the primary right in a democracy'[495] and the basis for many other fundamental freedoms. The right is protected in all the key human rights instruments including Article 19 of the International Covenant on Civil and Political Rights and Article 10 of the European Convention on Human Rights. Freedom of expression is also protected in most domestic constitutions,[496] including the Irish Constitution, with the First Amendment of the US Constitution offering a particularly strong protection for the right.[497]

Traditionally, the ECtHR strongly defends the right to freedom of expression, with the Court stating that 'freedom of expression constitutes one of the essential foundations of a democratic society and one of the basic conditions for its progress and each individual's self-fulfilment'.[498] Freedom of expression not only applies to 'information or ideas that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population.'[499]

Organizations such as the ACLU, Electronic Frontier Foundation and other free speech advocates argue that laws addressing IBSA may violate the right to freedom of expression.[500]

> We oppose laws with little regard for the risks for legitimate speech. We believe that the provision of technical tools such as filters, blocklists, and reporting mechanisms, when under the control of users, can be more effective than blanket laws or policies that attempt to regulate speech, as well as being less capable of misapplication that could, in turn, infringe on the free expression rights of speakers.[501]

---

[494] Layla Goldnick, 'Coddling the Internet: How the CDA Exacerbates the Proliferation of Revenge Porn and Prevents a Meaningful Remedy for its Victims' (2015)21 Cardozo Journal of Law & Gender 583.
[495] See Tom Daly, 'Strengthening Irish Democracy: A Proposal to Restore Free Speech to Article 40.6.1°(I) of the Constitution' (2009) 31(1) Dublin University Law Journal 228, referring to the judgment of Lord Steyn in R v S secretary of State for the Home Department, ex p Simms [2000] 2 AC 115 at 126.
[496] Freedom of expression is protected under the Irish Constitution under Article 40.6.1.
[497] The First Amendment to the US Constitution provides: 'Congress shall make no law respecting an establishment of religion or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.'
[498] *Handyside v United Kingdom* (1979-1980) 1 EHRR 737 at paragraph 49.
[499] ibid.
[500] Electronic Frontiers, Submission, Content Regulation in the Digital Age (2 February 2018) < https://www.ohchr.org/Documents/Issues/Opinion/ContentRegulation/EFF.pdf> accessed 20 February 2022; Michelle Daniels, 'Chapters 859 & 863: Model Revenge Porn Legislation or Merely a Work in Progress?' (2014) 46 McGeorge Law Review 297.
[501] Electronic Frontiers, Submission, Content Regulation in the Digital Age (2 February 2018) < https://www.ohchr.org/Documents/Issues/Opinion/ContentRegulation/EFF.pdf> accessed 20 February 2022.

Furthermore, Facebook states that the limitation of speech involved in forcing intermediaries to remove harmful content will lead to over-monitoring and removal of content, therefore amounting to infringements on freedom of expression.[502] Twitter also expressed concern in its 2018 transparency report that new legislation and ongoing regulatory discussions taking place globally about online content will have 'a potential chilling effect with regards to freedom of expression.'[503]

On the other hand, many stakeholders within the Irish context including political representatives; NGOs such as Children's Rights Alliance and the Irish Society for the Prevention of Cruelty to Children; the Ombudsman for Children; and the Law Reform Commission have advocated for increasing the accountability of intermediaries in relation to harmful online content. [504] The Association for Progressive Communications in Australia released a report that examined the policies of Facebook, Twitter and YouTube, and discovered that all three intermediaries lacked transparency around reposting and redress processes and that they had no commitment to upholding human rights standards other than the endorsement of free speech.[505] The report further stated that these platforms have 'erred on the side of unrestrained expression, often to women's detriment'.[506]

Balancing the right to privacy and the right to freedom of expression is challenging. However, decisions by the ECtHR have taken a more 'circumscribed approach to freedom of expression in favour of upholding the right to privacy'.[507] When drafting legislation that tackles the challenge of IBSA, it is necessary to fully consider privacy as well as free expression.[508]

---

[502] On the 1st of August 2018 the Joint Committee on Communications, Climate Action and Environment held a discussion on the moderation of violent and harmful content on the Facebook platform. Niamh Sweeney, head of public policy at Facebook Ireland and Siobhán Cummiskey, Facebook's head of content policy for Europe, the Middle East and Africa attended the meeting.

[503] Twitter Public Policy, 'Expanding and building #TwitterTransparency' (5th April 2018) < https://blog.twitter.com/en_us/topics/company/2018/twitter-transparency-report-12.html > accessed 20 February 2022; Digital Desk 'Warning over chilling impact on 'freedom of expression' if social media regulation unchecked' *Irish Examiner* (Dublin, 6 April 2018);Tom Whitehead, 'Twitter cases threat to freedom of speech' *The Telegraph* (London, 3 February 2013).

[504] Tim O'Brien, 'Cyberbullying watchdog office should open without delay' *Irish Times* (Dublin, 29 March 2018); Ronán Duffy, 'Calls for fines and gardaí after undercover report about Facebook moderation in Dublin' *The Journal* (18 July 2018).

[505] Carly Nyst, *End Violence: Internet Intermediaries and Violence against Women Online* (Executive Summary and Findings, Association for Progressive Communications, July 2014) 3.

[506] ibid.

[507] Law Reform Commission, Harmful Communications and Digital Safety (LRC 116 — 2016) para 1.56

[508] Liz Halloran, 'Race to Stop 'Revenge Porn' Raises Free Speech Worries' (NPR, 6th March 2014) < https://www.npr.org/sections/itsallpolitics/2014/03/06/286388840/race-to-stop-revenge-porn-raises-free-speech-worries?t=1645387722719 > accessed 20 February 2022.

> While it is imperative that intermediaries respond to the nonconsensual distribution of intimate images, it is also important that images of women's bodies uploaded with consent are not arbitrarily censored.[509]

One of the core challenges for intermediaries seeking to protect human rights on their platforms is the difficulty in developing processes that are both sufficiently responsive to abuse and sufficiently protective of freedom of expression.[510] Suzor, Seignior; and Singleton pointed out that in some cases consensually shared images of women's bodies are being removed from social media sites, including images of breastfeeding mothers, and indigenous women. Instead of protecting people, such actions suppress freedom of expression and are disempowering to women.[511] As a result, platforms must 'ensure that ordinary women are not prevented from sharing their images' due to overly censorious responses.[512]

1.7.2 Due process

Due process is interpreted as the right to be treated fairly, efficiently and effectively by the administration of justice. The right to due process places limitations on laws and legal proceedings to guarantee fundamental fairness and justice. Due process is interpreted in accordance with established and sanctioned legal principles and procedures and with safeguards in place for the protection of individual rights. The right to due process is governed by Article 38.1 of the Irish Constitution and Article 6 of the European Convention on Human Rights. Under current non-statutory, self-regulated arrangements, individuals can report harmful content to social media sites and request that it be removed.[513] All the prominent social media companies have content and conduct policies and standards that outline their approaches to various categories of harmful content, including the posting of private information without consent. In their operation, several of these policies lack consistency regarding what content the platforms remove, on what criteria are removal decisions made, and also whether appeal processes are available. Due process in the context of IBSA poses two challenges. Firstly, the self-regulation of social

[509] Nicolas Suzor, Bryony Seignior & Jennifer Singleton, 'Non-consensual porn and the responsibilities of online intermediaries' (2017) 40(3) Melbourne University Law Review 1057, 1097.
[510] ibid.
[511] Nicolas Suzor, Bryony Seignior & Jennifer Singleton, 'Non-consensual porn and the responsibilities of online intermediaries' (2017) 40(3) Melbourne University Law Review 1057, 1097; Georgie Keate, 'Facebook Removes "Offensive' Photo of Breastfeeding Mother', *The Times* (London, 30 October 2014); Leigh Alexander, 'Facebook's Censorship of Aboriginal Bodies Raises Troubling Ideas of 'Decency'', (*The Guardian*, 23 March 2016) < https://www.theguardian.com/technology/2016/mar/23/facebook-censorship-topless-aboriginal-women > accessed 20 February 2022.
[512] Nicolas Suzor, Bryony Seignior & Jennifer Singleton, 'Non-consensual porn and the responsibilities of online intermediaries' (2017) 40(3) Melbourne University Law Review 1057, 1097.
[513] Law Reform Commission, Harmful Communications and Digital Safety (LRC 116 — 2016) para 3.04

media platforms may hinder a suspected perpetrator's right to fair procedures as the offending content is often removed without any review process infringing on the individual's right to free speech. This concern was particularly highlighted in the Santa Clara principles.[514] This project engaged civil society organisations, industry representatives, policymakers and academic researchers to create a priority list for best practice to ensure transparency and accountability in the content moderation practices of social media platforms. The report also offers 'guidance to internet platforms on how to provide users with meaningful due process when their posts are taken down or their accounts are suspended, and to help ensure that the enforcement of company content guidelines is fair, unbiased, and respectful of users' free expression rights.'[515] The three principles urge companies to:

- publish the numbers of posts removed and accounts permanently or temporarily suspended due to violations of their content guidelines;
- provide clear notice to all users about what types of content are prohibited, and to each affected user about the reason for the removal of their content or the suspension of their account; and
- enable users to engage in a meaningful and timely appeals process for any content removals or account suspensions.[516]

1.8 Conclusion

This chapter introduced the key concepts, technologies, and terms which will be referenced throughout this thesis. Some specific issues were discussed in detail in order to provide a foundation for later discussions. Crucially, this chapter examined the concept and development of IBSA and demonstrated the important link between technology and the online world to the proliferation of IBSA. Understanding the scope of IBSA and the impact of technology in facilitating it is crucial as it provides a basis for the arguments made in Chapters 2-5 of this thesis and equips the reader with knowledge essential for the understanding of future discussions regarding legislative decisions and the effectiveness of enforcement responses. In particular, these discussions better inform the reader on the

[514] The Santa Clara Principles on Transparency and Accountability in Content Moderation < https://santaclaraprinciples.org/> accessed 20 February 2022.
[515] Internet Policy Observatory, 'The Santa Clara Principles on Transparency and Accountability of Content Moderation Practices' (2019) < http://globalnetpolicy.org/research/the-santa-clara-principles-on-transparency-and-accountability-of-content-moderation-practices/ > accessed 3 March 2019.
[516] The Santa Clara Principles on Transparency and Accountability in Content Moderation < https://santaclaraprinciples.org/> accessed 20 February 2022.

behaviours the Australian regulatory system examined in Chapters 2-3 are designed to target.

Specific legal issues raised in the online context were discussed. An understanding of these challenges provides the grounding for a more nuanced analysis of IBSA-targeted legislation in both Australia and Ireland. Furthermore, the challenge posed by difficulties of jurisdiction and anonymity highlight the need for alternative mechanisms of enforcement and harm mitigation in order to address the needs of victims. These are key issues considered when assessing the Australian and Irish approaches to the regulation of IBSA from a victim-centred perspective.

It was also important to acknowledge that IBSA is not an entirely new phenomenon but rather an act facilitated by the internet. The internet has increased its impact and potential harm to victims. Behaviours associated with IBSA, such as digital voyeurism and sextortion, were discussed to provide contextual understanding before analysing legislative responses in Chapters 2-5. Similarly, the discussion of the impact of IBSA on victims will facilitate a more informed evaluation of the appropriateness of penalties and the effectiveness of remedies in later chapters. It was also necessary to highlight the harm caused in order to illustrate the importance of effective action in this area.

This chapter outlined how existing civil and criminal laws fail to fully address the challenge of IBSA and how the remedies under these actions can be inaccessible to victims of IBSA due to cost, lack of know-how, and potential re-traumatising effects. Moreover, the time in which it takes for legal proceedings to result in the removal of content can be another barrier to effectiveness where the prompt removal of the IBSA image is often the priority of victims.

While victim-blaming attitudes persist in some contexts, this chapter has discussed how these attitudes appear to have lessened in recent years as support for IBSA legislation has grown in many jurisdictions.

Chapter 2: Australia's regulatory response to image-based sexual abuse: Desk-based analysis of the Office of the eSafety Commissioner

2.1 Introduction

A key aim of this thesis is to consider appropriate enforcement responses to the issue of image based sexual abuse (IBSA) from a victim-centred perspective. Australian legislators have been active in responding to the growing prevalence of IBSA. All eight states and territories have passed criminal laws against the non-consensual sharing of sexual images or videos and the Parliament of Australia also criminalised IBSA in 2018. With the establishment of the Office of the eSafety Commissioner (OESC) in 2015,[1] Australia has been a pioneer in tackling the challenges of online enforcement with innovative regulatory approaches. The OESC has played an increasingly important role in the Australian response to IBSA. Chapter 3 describes and draws insights from interviews conducted with Australian experts familiar with the operation of the OESC, but it is first necessary to conduct a desk-based analysis of the structure, powers, and operation of the regulatory body. Since the conducting of the interviews discussed in Chapter 3, new legislation has been implemented in Australia under the Online Safety Act 2021 which commenced on the 23rd of January 2022. The interviews discussed in Chapter 3 are based on the governing legislation of the OESC at the time the interviews were conducted which was the Enhancing Online Safety Act 2015 and amending acts. As a result, this chapter explains and assesses the legislation relevant at the time the interviews were conducted. Setting out the development of the regime as it was at the time of the interviews is essential as it forms the basis of the interviews discussed in Chapter 3. Furthermore, there is a wealth of insight to be gained from examining the functioning of the OESC under the prior legislative framework due to the availability of rich resources like the OESC annual reports covering that period of time. Understanding the functioning of the OESC prior to the newly implemented legislation provides valuable

[1] The eSafety Commissioner was established under the Enhancing Online Safety Act 2015. The OESC was previously called the Office of the Children's eSafety Commissioner as the role of the Commissioner was to protect children online. In 2017, the Act was amended to expand the Commissioner's remit to promoting and enhancing online safety for all adults. In 2021, the Online Safety Act 2021 was implemented which is now the current governing legislation of the Office of the eSafety Commissioner.

insights which will inform the authors assessment of the Irish regulatory approach in Chapter 4 and 5.

Representatives from the Australian Government and Non-Governmental Organisations have recognised the importance of addressing victim needs in the Australian context. For example, Member of Parliament and Committee Chair of the Select Committee on Social Media and Online Safety, Lucy Wicks stated that 'the Australian Government is leading the world in online safety, but technology and online predators evolve quickly, so the Government must continue to hold social media companies to account and support victims of abuse'.[2] The Alannah and Madeline Foundation stated that there is a need for 'targeted interventions' to address 'young people's needs'.[3] The Alannah and Madeline Foundation also stated that 'States parties should listen to their [victims of online harm] needs and give due weight to their views'.[4] In adopting a victim-centred approach, this thesis identifies the key needs of victims of IBSA and the key tools/mechanisms that may address these needs. This chapter is where the foundation of the victim-centred approach of this thesis is set out. The victim-centred framework is represented as a table later in this chapter and is further refined and refracted throughout the thesis as a framework for analysis when assessing the effectiveness of the Australian and Irish responses to IBSA.

First, this chapter begins with an overview of the issue of IBSA in the Australian context. A discussion of the prevalence of IBSA, policies developed, and laws introduced in response, and the associated enforcement challenges highlight the extent of the problem for Australian victims, communities, courts, and police and provides insight into the issues the OESC is designed to address. Identifying these issues provides context when discussing the needs of IBSA victims when seeking redress which will be discussed in section 2.6.

Second, this chapter maps out the development of the OESC from its role of solely protecting children online to its expanded role of 'promoting and enhancing online safety for all Australians'.[5] For the purposes of this chapter, this author adopts a victim-centred approach by paying particular attention to the OESC role in protecting victims of IBSA.

---

[2] Lucy Wicks, 'Social Media and Online Safety Report Finds Serious Levels of Online Harm'(Parliament of Australia Media Release, 15 March 2022).
[3] Alannah and Madeline Foundation, 'Inquiry into Social Media and Online Safety Submission' (December 2021).
[4] ibid.
[5] eSafety Commissioner, 'Our Legislative Functions' <https://www.esafety.gov.au/about-us/who-we-are/our-legislative-functions> accessed 15 June 2020.

Understanding how the remit of the OESC has developed over time highlights past limitations which can inform the discussion of creating an Irish body with a similar function as examined in Chapter 5. Within this discussion, the functions of the OESC as they were at the time the interviews were conducted are outlined with particular attention afforded to its innovative remediation powers under the Cyberbullying Complaints Scheme, the Online Content Scheme, and the IBA Portal.

Once the functions, powers and structure of the OESC are clearly established, this chapter considers the impact and operation of the OESC in practice through a victim-centred lens, in order to assess its merits and limitations in meeting the needs of victims. This is conducted through an examination of the governing legislation in place at the time the interviews were conducted (The Enhancing Online Safety Act 2015) and other key documents such as the OESC Annual Reports and the Briggs Report. This chapter provides a preliminary assessment of the OESC in the context of IBSA based on published evidence. The insights gained in this chapter inform the issues to be explored through semi-structured interviews with experts as discussed in Chapter 3.

Next, this chapter provides an overview of the Online Safety Act 2021 which is the current governing legislation of the OESC. In particular this section sets out the key provisions of the Online Safety Act which are relevant to IBSA. This section notes how the new law changes the powers and structure of the OESC as discussed in previous sections of the chapter. Understanding the current legislation will allow the author to assess how the new law impacts on issues raised in the interviews discussed in Chapter 3. Furthermore, understanding the new powers of the OESC in the context of IBSA will provide an additional point of comparison for Chapter 5 when assessing the Irish regulatory response.

Finally, this chapter builds on its analysis of the Australian laws by reviewing key academic literature considering the Australian context in order to identify the key components of a victim-centred approach. These components are used to develop a framework upon which to assess legislative and policy approaches to IBSA in Chapter 3, Chapter 4, and Chapter 5.

The Australian approach prior to the newly enacted Online Safety Act 2021 has previously been considered by the Irish Law Reform Commission (LRC) in a report

outlining proposed laws for the regulation of harmful communications and digital safety.[6] Indeed, numerous influential Irish reports—including the LRC report,[7] a report from the Oireachtas Committee on Children and Youth Affairs,[8] and a Joint Committee on Tourism, Culture, Arts, Sport and Media Report on the Pre-Legislative Scrutiny of the General Scheme of the Online Safety and Media Regulation Bill[9]—endorse the establishment of a Digital Safety Commissioner/Online Safety Commissioner influenced by the model provided by the Australian OESC. Combined with the insights gained from Chapter 3 and a refracted victim-centred framework, the understanding gained in this chapter will be used in Chapter 5 of this thesis in order to assess the best approach for Ireland.

2.2 The extent of the problem of image-based sexual abuse in Australia

The increased prevalence of non-consensual sharing of intimate images around the globe is in large part due to the 'pervasive ubiquity of social media' as well as the omnipresence of mobile phones and other digital recording devices.[10] The ubiquity of such devices greatly increases the opportunities for capturing images and videos without consent and sometimes without the knowledge of the person targeted.[11] Whether the images are initially captured with or without consent, significant risks arise where one party intends the images to be private.[12] This risk is magnified due to the readily reproducible and shareable nature of digital images. Risks remain even where both parties intend the images to be private due to the security vulnerabilities associated with online communications and data storage.[13]

---

[6] Law Reform Commission, *Harmful Communications and Digital Safety* (LRC 116 — 2016).
[7] ibid.
[8] Houses of the Oireachtas, Joint Committee on Children and Youth Affairs, *Report on Cyber Security for Children and Young Adults* (32 CYA 011 — March 2018)
[9] Joint Committee on Tourism, Culture, Arts, Sport and Media, *Report of the Joint Committee on the Pre-Legislative Scrutiny of the General Scheme of the Online Safety and Media Regulation Bill* (TCASM/21/07 — November 2021).
[10] Senate Legal and Constitutional Affairs References Committee, Parliament of Australia, *Phenomenon Colloquially Referred to as 'Revenge Porn'* (2016) 3.
[11] 86% of Australian households have access to the internet. See Australian Bureau of Statistics, Household Use of Information Technology, Australia, 2016- 17, < http://www.abs.gov.au/ausstats/abs@.nsf/mf/8146.0 > accessed 10 May 2018. In 2015, 93% of Australian adults use mobile phones and 80% of Australians use their mobile phones to access the internet. See Australian Communications and Media Authority, *Communications Report* (2014-15) 21.
[12]Nicola Henry & Anastasia Powell, 'Beyond the 'sext': Technology facilitated sexual violence and harassment against adult women' 48(1) Australian & New Zealand Journal of Criminology (2015) 104.

IBSA has been identified as an issue of growing concern in Australia. This is reflected in several studies assessing the level of IBSA in Australian society. In 2014, Powell and Henry conducted a survey of 3000 Australians aged between 18-54. The survey found that one in 10 respondents reported that an intimate image of them had been distributed without their consent and one in 10 respondents also reported that someone took an intimate image of them without consent. Furthermore, 9.6 per cent of respondents reported that someone had threatened to post an intimate image of them.[14] The Domestic Violence Resource Centre in Victoria conducted a national survey in 2015 with 546 domestic violence workers in Australia. Of the 546 domestic violence workers surveyed, 98 per cent reported that their clients had experienced the 'non-consensual sharing of intimate images and/or technology facilitated stalking and abuse'.[15] Powell, Henry, and Flynn conducted another survey in 2016 to gather further data on the prevalence of IBSA within Australia. The researchers conducted a national survey with 4274 Australians aged between 16 to 49 years. Results revealed that one in 10 respondents experienced the dissemination of their intimate image without consent. Furthermore, it was found that one in five respondents experienced at least one form of IBSA, including the dissemination of intimate images without consent, an intimate image taken without consent or the threat to disseminate an intimate image.[16] Powell, Henry, and Flynn discovered that one in 10 women reported someone taking an image of their cleavage without their permission (colloquially known as 'downblousing') and one in 20 women reported someone taking an image directed underneath their skirt (colloquially known as 'upskirting') without their permission. Henry, Flynn, and Powell also reported on perpetration levels in their 2016 survey.[17] The survey found that one in 10 respondents engaged in at least one form of

---

[14] Anastasia Powell & Nicola Henry, *Digital Harassment and Abuse of Adult Australians. A Summary Report.* (Melbourne: RMIT University, 2015). This study survey 3000 Australians aged 18-54.

[15]Elizabeth Snell, Law Reform and Policy Coordinator, Women's Legal Services NSW, *Committee Hansard*, (2016) 27.

[16] Nicola Henry, Asher Flynn & Anastasia Powell, *Not just 'revenge pornography': Australians' experiences of image-based sexual abuse: A summary report* (Melbourne: RMIT University, 2017). The researchers conducted a national survey with 4274 Australians aged between 16 – 49 years. The study noted that the prevalence rates presented in the survey only included cases where victims became aware that someone took or shared an intimate image of them without consent. Therefore, the rate of victimisation may be higher as some victims may be unaware that an intimate image of them has been taken or disseminated. The survey forms part of a larger project. See Nicola Henry, Asher Flynn and Anastasia Powell, 'Responding to 'revenge pornography': Prevalence, nature and impacts' (2019) Report to the Criminology Research Advisory Council Grant: CRG 08/15-16.

[17] Nicola Henry, Asher Flynn & Anastasia Powell, 'Responding to 'revenge pornography': Prevalence, nature and impacts' Report to the Criminology Research Advisory Council Grant: CRG 08/15-16 (March 2019). The survey part of this research was conducted in 2016. The survey sample comprised of 4,274 Australian respondents, aged 16 to 49 years with quota sampling across gender, age and sexuality to approximate the demographics representative of the Australian population (as per the Australian Bureau of Statistics (ABS) Census data).

IBSA behaviour. Almost nine per cent of survey respondents disclosed that they had taken an intimate image of another person without consent, and nearly seven per cent disclosed they had distributed an intimate image without consent. One in 20 respondents disclosed that they made threats to another person claiming they would distribute their intimate image(s).[18] In 2017, the OESC conducted a survey of 4122 Australian adults. The survey discovered that one in 10 respondents had had their intimate image shared without consent. In another survey conducted in 2017 by the University of Plymouth, Net Safe, Safer Internet Centre, and the OESC, out of 1424 Australian teens aged 14-17, one in three had some experience with 'sexting'. More recently, findings from a cross-national survey conducted by Henry, Powell, Scott, and Flynn in 2019 suggest that IBSA has increased in prevalence. The 2019 study found that one in five respondents had had their intimate image disseminated without consent. One in three respondents reported having their intimate image taken without consent and one in five reported being threatened to have their intimate image shared.[19] These studies demonstrate the pervasiveness of IBSA within Australia.

Australian Internet safety campaigns – such as the 'ThinkUKnow' campaign and the New South Wales' 'Safe Sexting: No Such Thing' campaign – highlight the issue of IBSA with an aim to raise awareness of the growing problem in order to suppress its growth.[20] The 'ThinkUKnow' campaign affords particular attention to explicit 'sexting' and 'selfies', flagging these acts as a major concern for Australia.[21] The campaign advises young people about the 'permanence' of their 'digital footprint' and the damaging impact that these behaviours can have on their social reputation.[22] The New South Wales' 'Safe

[18] Nicola Henry, Asher Flynn & Anastasia Powell, 'Responding to 'revenge pornography': Prevalence, nature and impacts' Report to the Criminology Research Advisory Council Grant: CRG 08/15-16 (March 2019).
[19] ibid.
[20] The 'ThinkUKnow' campaign is led by the Australian Federal Police. The ThinkUKnow campaign is delivered nationally in partnership with law enforcement and industry to raise awareness about the safety of young people online. ThinkUKnow , < https://www.thinkuknow.org.au/ > accessed 24 February 2022. See also 'Start the Chat' which a National Online Safety Awareness campaign is funded by the Australian Government and led by the eSafety Commissioner. 'Start the Chat' is designed to help anyone (particularly parents, carers, and teachers) who are around children aged 5 to 18 to understand the importance of starting the chat about online safety with young people. See https://www.esafety.gov.au/sites/default/files/2019-09/Start%20the%20Chat%20and%20Stay%20Safe%20Online%20-%20Booklet.pdf
[21]As discussed in chapter 1 section 1.4.3, 'sexting' and 'selfies' are colloquial terms. 'Sexting' is the practice of sending sexually explicit text messages or images both still and video, including nude or semi-nude photographs, via a device or over the internet. 'Selfies' Selfies are defined as a self-shot photograph, taken at arms-length or in front of a mirror.
[22]Nicola Henry & Anastasia Powell, 'Beyond the 'sext': Technology facilitated sexual violence and harassment against adult women' 48(1) Australian & New Zealand Journal of Criminology (2015) 104.

Sexting: No Such Thing'[23] campaign also highlights the legal ramifications associated with the dissemination of intimate images by young people. Such issues include the risk of being added to a sex offenders register under Australian Criminal Law[24] and the possibility of being associated with the creation and distribution of explicit images of children where the subject of the image is under the age of consent.[25]

In response to the growing problem of IBSA, legislation addressing the issue has been introduced at both federal and state/territory levels. IBSA may be prosecuted at the federal level under section 474.17(A) of the Criminal Code Act 1995 as amended by the Enhancing Online Safety Act (Non-Consensual Sharing of Intimate Images) Act 2018. Section 474.17 of the Criminal Code Act prohibits the use of a carriage service[26] in a way that a reasonable person would regard as being menacing, harassing or offensive.[27] This offence carries a penalty of three years imprisonment. The Enhancing Online Safety Act (Non-Consensual Sharing of Intimate Images) Act 2018 amended the Criminal Code Act 1995 to include section 474.17A(1) which created an aggravated offence for using a carriage service to menace, harass or cause offence by transmitting, making available, publishing, distributing, advertising or promoting private sexual material.[28] The Act defines 'private sexual material' as including:

(a) material that:

---

[23] Australia's New South Wales Government launched an education campaign combat the growing practice of sexting through a fact sheet for schools, parents and youngsters to warn about the possible lifetime consequences of sexting. Safe Sexting: No Such Thing < https://www.rutherfordschools.org/media/it/onlinesafety/sextingfacts.pdf> accessed 13 January 2022.

[24] The Criminal Code Act 1995, Part 10.6 Subdivision D states 'it is an offense to access, transmit, publish, process, control, supply or obtain child pornography' where a child is considered persons under the age of 18 or who appear to be under the age of 18.

[25]Nicola Henry & Anastasia Powell, 'Beyond the 'sext': Technology facilitated sexual violence and harassment against adult women' 48(1) Australian & New Zealand Journal of Criminology (2015) 104. The age of consent is 16 years of age in the Australian Capital Territory, New South Wales, Northern Territory, Queensland, Victoria and Western Australia. (*Crimes Act 1900 (ACT), s 55; Crimes Act 1900* (NSW), s 66C; *Criminal Code Act 1983 (NT), s 127*; *Criminal Code Act 1899 (*QLD), s 215; *Crimes Act 1958* (VIC), s 45; *Criminal Code Act Compilation Act 1913* (WA), s 321. In Tasmania and South Australia, the age of consent is 17 years of age. (*Criminal Code Act 1924* (TAS), s124; *Criminal Law Consolidation Act 1935(* SA), s49.

[26] '"Carriage service" means a service for carrying communications by means of guided and/or unguided electromagnetic energy'. Telecommunications Act 1997.

[27] Criminal Code Act 1995, s 474.17(1) states: (1) A person commits an offence if: (a) the person uses a carriage service; and (b) the person does so in a way (whether by the method of use or the content of a communication, or both) that reasonable persons would regard as being, in all the circumstances, menacing, harassing or offensive. Penalty: Imprisonment for 3 years.

[28] Criminal Code Act 1995, s 474.17A(1) states: (1) A person commits an offence against this subsection if: (a) the person commits an offence (the ***underlying offence***) against subsection 474.17(1); and (b) the commission of the underlying offence involves the transmission, making available, publication, distribution, advertisement or promotion of material; and (c) the material is private sexual material. Penalty: Imprisonment for 5 years.

(i) depicts a person who is, or appears to be, 18 years of age or older and who is engaged in, or appears to be engaged in, a sexual pose or sexual activity (whether or not in the presence of other persons); and
(ii) does so in circumstances that reasonable persons would regard as giving rise to an expectation of privacy; or

(b) material the dominant characteristic of which is the depiction of:
(i) a sexual organ or the anal region of a person who is, or appears to be, 18 years of age or older; or
(ii) the breasts of a female person who is, or appears to be, 18 years of age or older; where the depiction is in circumstances that reasonable persons would regard as giving rise to an expectation of privacy.[29]

This offence carries a maximum sentence of five years imprisonment. Furthermore, section 474.17A(4) provides for a special aggravated offence whereby a person who commits an offence under section 474.17A(1) has more than three civil penalty orders made against them by the OESC.[30] This offence carries a maximum sentence of seven years imprisonment.

It is notable that all eight states/territories have enacted criminal laws that address IBSA.[31] In 2013, South Australia became the first state to criminalise IBSA under the Summary Offences (Filming Offences) Amendment Act 2013 which amended the Summary Offences Act 1953. Section 26C creates an offence for distributing an 'invasive image' of another person, knowing or having reason to believe that the other person does not consent to the distribution of the image.[32] Section 26D governs the threat to disseminate an invasive image whereby there is a reasonable belief that this threat would be carried out.[33] In 2014, Victoria introduced legislation which makes it an offence to threaten to distribute or distribute an intimate image introduced under Section 41D A and 41D B of the Summary Offences Act 1966 as amended by the Crimes Amendment (Sexual Offences and Other Matters) Act 2014. [34] In August 2017, New South Wales introduced three new criminal offences related to IBSA behaviour: recording intimate images

[29] Criminal Code Act 1995, s 472.1.
[30] Criminal Code Act 1995, s 474.17A(4) states: (4) A person commits an offence against this subsection if: (a) the person commits an offence (the ***underlying offence***) against subsection 474.17(1); and (b) the commission of the underlying offence involves the transmission, making available, publication, distribution, advertisement or promotion of material; and (c) the material is private sexual material; and (d) before the commission of the underlying offence, 3 or more civil penalty orders were made against the person under the Regulatory Powers (Standard Provisions) Act 2014 in relation to contraventions of subsection 44B(1) of the Enhancing Online Safety Act 2015. Penalty: Imprisonment for 7 years.
[31] Tasmania currently lacks the type of targeted law that the other states/territories have which directly criminalise IBSA. However, Tasmania have made amendments that address some acts of IBSA through the Criminal Code Amendment Bullying Act 2019 which amends the Criminal Code Act 1924 to extend the criminal offence of stalking to include the publishing or transmitting of offensive material.
[32] Summary Offences Act 1953 (SA), s 26C.
[33] ibid s 26D.
[34]Crimes Amendment (Sexual Offences and Other Matters) Act 2014 (VIC), s 41DA & s 41DB.

without consent; distributing intimate images without consent; and threatening to record or distribute intimate images under the Crimes Act 1900 (NSW) as amended by the Crimes Amendment (Intimate Images) Act 2017.[35] In 2017, Australian Capital Territory or 'Canberra' implemented targeted legislation against IBSA under the Crimes (Intimate Image Abuse) Amendment Act 2017 as an amendment to the Crimes Act 1900 (ACT). Offenders who disseminate or threaten to disseminate an intimate image may receive a sentence of up to three years imprisonment or a $45,000 fine. The penalty increases to up to five years or a fine of $75,000, if the victim is less than sixteen years of age.[36] In 2018, the Northern Territory introduced the Criminal Code Amendment (Intimate Images) Act 2018 which amended the Criminal Code Act 1983 (NT). Part VI Division 7A of the Criminal Code Act 1983 (NT) (specifically Sections 208AB and 280AC) creates two new offences. These include an offence to intentionally distribute an intimate image of another person, if the other person did not consent to the distribution and the distributor was reckless as to that fact and an offence to intentionally threaten to distribute an intimate image of another person, intending that the other person fear that the threat be carried out.[37] In 2018, Queensland also implemented targeted legislation to combat IBSA through the Criminal Code (Non-consensual Sharing of Intimate Images) Amendment Act 2018 which amended the Criminal Code Act 1899 (Qld). Two offences were created including an offence to distribute an intimate image without consent under Section 223 and the threat to distribute an intimate image under Section 229A.[38] In 2019, Western Australia introduced the Criminal Law Amendment (Intimate Images) Act 2018 (WA) which inserted a new Section 221BD(2) into the Criminal Code Act 1913 (WA). This provision makes it an offence to distribute an intimate image of another person without consent and is punishable by a penalty of three years imprisonment, or a summary conviction penalty of 18 months and a fine of $18000.[39] Finally, in 2019 Tasmania passed the Criminal Code Amendment Bullying Act 2019 amending the Criminal Code Act 1924 to extend the criminal offence of stalking to include the publishing or transmitting of offensive material.[40]

[35] Crimes Act 1900 (NSW), s 91P, s 91Q, s 91R.
[36] Crimes Act 1900 (ACT), s 71A.
[37] Criminal Code Act 1983 (NT), s 208AB, s 280AC.
[38] Criminal Code Act 1899 (Qld) s 223, s 229A.
[39] The Criminal Code Act 1913 (WA) s 221BD (2).
[40] Criminal Code Act 1924 (TAS), s 192(1).

Law reform efforts in New South Wales and the Australian Capital Territory have been described as 'exemplary in an international context'.[41] However, in terms of capturing the harms associated with IBSA, Tasmania, Western Australia, South Australia, and Victoria have been less effective. Importantly, New South Wales and the Australian Capital Territory do not require intent to cause distress or harm, and as such capture a range of perpetrators regardless of their motivation. South Australia and Victoria require the perpetrator to intend to disseminate the image in question. An image which is disseminated due to recklessness is not protected under these laws. The lack of consideration for reckless posting of intimate images leaves an easy loophole for perpetrators.[42] While the Victorian legislation, for example, defines 'intimate image' as 'a moving or still image that depicts (a) a person engaged in sexual activity; (b) a person in a manner or content that is sexual; or (c) the genital or anal region of a person, or, in the case of a female, the breasts', Western Australia has no definition of an intimate image.

In a qualitative study conducted by Henry, Flynn, and Powell, it was discovered that there is strong support from stakeholders within Australia for the introduction of consistent state/territory laws that criminalise IBSA.[43] The current legislative frameworks within Australia used to target IBSA are said to 'not sufficiently accommodate the intent, magnitude, and range of harms' that are committed through offensive behaviours involving intimate images.[44] The lack of uniformity between jurisdictions — such as the wide use of terms including 'intimate images', 'private sexual material', 'invasive images', and 'intimate personal images — has resulted in a number of problems for law enforcement and prosecution agencies.[45]

[41] Nicola Henry, Asher Flynn & Anastasia Powell, 'Responding to 'Revenge Pornography': Prevalence, Nature and Impacts' Report to the Criminology Research Advisory Council Grant: CRG 08/15-16 (March 2019).
[42] Franks M.A, *Drafting an Effective "Revenge Porn " Law: A Guide for Legislator* (Cyber Civil Right Initiative, 2 November 2015) 3.
[43] Nicola Henry, Asher Flynn & Anastasia Powell, 'Responding to 'revenge pornography': Prevalence, nature and impacts' Report to the Criminology Research Advisory Council Grant: CRG 08/15-16 (March 2019).
[44] Law Reform Committee, Parliament of Victory, 'Inquiry into Sexting' *Report of the Law Reform Committee for the Inquiry into Sexting* (Parliamentary Paper No. 230, Session 2010-2013) 140.
[45] Nicola Henry & Anastasia Powell 'Beyond the 'sext': Technology facilitated sexual violence and harassment against adult women' (2015) 48(1) Australian & New Zealand Journal of Criminology 104.

While targeted legislation has expressive value, sending a signal to society that IBSA is a serious crime and not the fault of the victim,[46] increased criminalisation has not automatically led to effective enforcement.[47] In Victoria, for example, police data revealed that between 1 January 2015 and 18 July 2017, there was 415 cases (62 arrests) of non-consensual distribution of an intimate image (Summary Offences Act 1966 (Vic) 41DA) and 144 cases (52 arrests) of threatening to distribute an intimate image (Summary Offences Act 1966 (Vic) 41DB). As the population of Victoria is over 6.6 million people,[48] these figures are 'suggestive of a level of ineffectiveness which is likely connected to challenges in policing'.[49] Laughton highlights that issues remain in tackling IBSA in Australia and that greater research is required in order to identify these challenges.[50] Challenges to effective enforcement include barriers to victim reporting, issues around anonymity, jurisdictional challenges, and issues with law enforcement resources and adequate training.

Police struggle to investigate complaints of IBSA. Resource restrictions and lack of technical skill and knowledge hinder the procuring of sufficient evidence.[51] Furthermore, the police sometimes fail to obtain the necessary co-operation of internet intermediaries.[52] The lack of evidence often leaves the police limited in taking further action in cases.[53] In a 2018 study conducted by Powell and Henry, participants explained that there is a lack of knowledge among the police when dealing with victims of IBSA.[54] A number of

[46] Erika Rackley & Clare McGlynn, 'The law must focus on consent when it tackles revenge porn' (*The Conversation,* 23 July 2014) < https://theconversation.com/the-law-must-focus-on-consent-when-it-tackles-revenge-porn-29501 > accessed 24 February 2022.
[47] Nicola Henry, Asher Flynn & Anastasia Powell, 'Policing image-based sexual abuse: stakeholder perspectives' (2018) 19 Police Practice and Research 565.
[48] Australian Bureau of Statistics, 'Australian Demographic Statistics' (2019) <https://www.abs.gov.au/AUSSTATS/abs@.nsf/DetailsPage/3101.0Mar%202019?OpenDocument> accessed 16 June 2020
[49] Nicola Henry, Asher Flynn & Anastasia Powell, 'Responding to 'Revenge Pornography': Prevalence, Nature and Impacts' Report to the Criminology Research Advisory Council Grant: CRG 08/15-16 (March 2019).
[50] Victoria Laughton, Research and Advisory Officer, Victim Support Service, Committee Hansard 7; The Senate, Legal and Constitutional Affairs References Committee, *Phenomenon colloquially referred to as 'revenge porn'* (February 2016).
[51] Anastasia Powell & Nicola Henry, 'Policing Technology-Facilitated Sexual Violence Against Adult Victims: Police and Serve Sectors Perspectives' (2016) 28(3) Policing and Society.
[52] Nicola Henry, Asher Flynn & Anastasia Powell, 'Responding to 'Revenge Pornography': Prevalence, Nature and Impacts' Report to the Criminology Research Advisory Council Grant: CRG 08/15-16 (March 2019).
[53] Office of the eSafety Commissioner, *Image-Based Abuse Qualitative Research Summary* (October 2017); Nicola Henry, Asher Flynn & Anastasia Powell, 'Policing image-based sexual abuse: stakeholder perspectives' (2018) 19 Police Practice and Research 565, 571.
[54] Anastasia Powell & Nicola Henry, 'Policing Technology-Facilitated Sexual Violence Against Adult Victims: Police and Serve Sectors Perspectives' (2016) 28(3) Policing and Society.301. In total, 30 stakeholder interviews were conducted in three Australian state jurisdictions. These comprised of 12 interviews with police members, 8 interviews with legal services stakeholders; and 10 interviews with

participants in this 2018 study noted that the police advised them that there was 'nothing they could do' and that they appeared to have little knowledge or awareness of the applicable laws.[55] Research commissioned by the eSafety Commissioner also mirrored these results showing that victims were often not believed or were told there was 'nothing' the police could do.[56] There appears to be a lack of awareness among some police of the harms to victims or the existence of laws on IBSA.[57]

Many cases of IBSA remain unreported. Research conducted by the OESC shows only one in four victims take action.[58] Surveys show that many victims are unaware that IBSA is a crime.[59] Moreover, in a study conducted by Henry, Flynn, and Powell between April 2016 and October 2017 with 44 stakeholders, participants identified a range of challenges that hindered victims from reporting IBSA to police. A consistent reason for the lack of reporting by victims was the fear of victim-blaming and the perceived lack of appreciation for the significance of the harm by law enforcement personnel.[60] Victims often avoid seeking redress because of the 'stigma attached to IBSA' and for fear that they will 'exacerbate' the situation.[61] In many cases victims were reluctant to share their images with police and as a result did not report the behaviour.[62] This suggests that the traditional route of reporting to the police may not be the best avenue of redress for victims of IBSA.

---

domestic violence and sexual assault service sector stakeholders. The majority of stakeholder participants were female, although all eight male participants were police members.

[55] Anastasia Powell & Nicola Henry, 'Policing Technology-Facilitated Sexual Violence Against Adult Victims: Police and Serve Sectors Perspectives' (2016) 28(3) Policing and Society.

[56] Office of the eSafety Commissioner, *Image-Based Abuse Qualitative Research Summary* (October 2017).

[57] Clare McGlynn, Erika Rackley, Kelly Johnson, Nicola Henry, Asher Flynn, Anatasia Powell, Nicola Gavey & Adrian Scott, 'Shattering lives and myths: A report on image-based sexual abuse' (2019) *Project Report. Durham University; University of Kent*. This report draws on interviews with 25 victim-survivors of image-based sexual abuse and over 25 stakeholders, including police, policy-makers, lawyers and survivor organisations conducted over a six-month period in 2018

[58] Office of the eSafety Commissioner, *Image-Based Abuse Qualitative Research Summary* (October 2017). researched used an online survey conducted during the 8th – 21st May 2017.

[59] Anastasia Powell, Nicola Henry, Adrian Scott & Asher Flynn, *Image-based sexual abuse: An international study of victims and perpetrators. Summary Repor*t (February 2020). 45.7% of the 6109 surveyed respondents believed IBSA was a crime while 15.1% did not think it was a crime and 39.2% did not know.

[60] Nicola Henry, Asher Flynn and Anastasia Powell, 'Responding to 'revenge pornography': Prevalence, nature and impacts' Report to the Criminology Research Advisory Council Grant: CRG 08/15-16 (March 2019); Anastasia Powell & Nicola Henry, 'Policing technology-facilitated sexual violence against adult victims: police and service sector perspectives' (2018) 28 Policing and Society 301.

[61] Office of the eSafety Commissioner, *Image-Based Abuse Qualitative Research Summary* (October 2017). The eSafety Commissioner commissioned the Social Research Centre and academics from RMIT University to conduct the qualitative research component. 38 interviews were conducted with female victims of IBSA aged between 18 to 44 and stakeholders.

[62] Nicola Henry, Asher Flynn and Anastasia Powell, 'Responding to 'revenge pornography': Prevalence, nature and impacts' Report to the Criminology Research Advisory Council Grant: CRG 08/15-16 (March 2019).

One of the greatest challenges across all forms of online crimes is the identification of perpetrators which is often complicated by the challenges of jurisdiction as discussed in Chapter 1.[63] Anonymity can facilitate negative online behaviours, as it allows individuals to freely exhibit inappropriate behaviour and attitudes without the normal social repercussions. For IBSA, this issue includes challenges with identifying perpetrators but also website hosts who can be located anywhere in the world. In Australia, representatives from the police identified that they worked on cross-jurisdictional cases with external law enforcement agencies in relation to offences against children.[64] However, at times they would not investigate offences involving adults in a cross-jurisdictional context due to the complicated nature of conducting the investigation.[65] Similar results were found by research commissioned by the OESC where participants explained that police were helpful in cases of IBSA where the victim was a child but were unhelpful in cases where the victim was an adult.[66]

Overall, IBSA is prevalent in Australia. Despite the implementation of legislation, challenges remain with its enforcement. Police need greater training in how to deal with victims in a sensitive manner, further education in technical investigation skills, cross jurisdictional support, and better awareness of the constantly developing and emerging technologies used to assist crimes of IBSA.[67] These challenges highlight the need for an organisation that is technically equipped, knowledgeable in IBSA behaviours, capable of fostering relationships with intermediaries, and understanding of the harms caused to victims so to be able to provide ongoing support.

One of the most challenging issues associated with IBSA is the 'persistence of sexually explicit or intimate images in cyberspace post-distribution.'[68] As the internet enables re-blogging and reposting, it is often practically impossible to retract an image once it has been distributed. In many cases victims need recurring support and advice. This highlights the importance of a mechanism which assists in the removal of intimate images

[63] See Chapter 1 section 1.2.4.
[64] Nicola Henry, Asher Flynn and Anastasia Powell, 'Policing image-based sexual abuse: stakeholder perspectives' (2018) 19 Police Practice and Research 571.
[65] Nicola Henry, Asher Flynn and Anastasia Powell, 'Policing Image-Based Sexual Abuse: Stakeholder Perspectives' (2018) 19 Police Practice and Research 571; Anastasia Powell and Nicola Henry, 'Policing Technology-Facilitated Sexual Violence Against Adult Victims: Police and Serve Sectors Perspectives' (2018) 28 Policing and Society 301.
[66] Office of the eSafety Commissioner, *Image-Based Abuse Qualitative Research Summary* (October 2017) 9.
[67] Anastasia Powell and Nicola Henry, 'Policing Technology-Facilitated Sexual Violence Against Adult Victims: Police and Serve Sectors Perspectives' (2018) 28 Policing and Society 304.
[68] Anastasia Powell & Nicola Henry, 'Sexual Violence in the Digital Age: The Scope and Limits of Criminal Law' (2016) 25(4) Social & Legal Studies 397.

specifically while providing continual support and advice.[69] The OESC with its expanded powers to administer a civil penalty scheme through its IBSA portal can be regarded as a response to some of these challenges.

2.3 The Development of the Office of the eSafety Commissioner

2.3.1 Introduction to the Office of the eSafety Commissioner

The OESC is an independent statutory office, supported by the Australian Communications and Media Authority (ACMA).[70] Julie Inman Grant is the current Commissioner and was appointed on the 23rd of November 2016. The eSafety Commissioner has the important role of 'leading, coordinating, and advising' on online safety issues to ensure 'safe, positive, and empowering' online experiences.[71] The eSafety Commissioner is a 'national leader'[72] on issues of online safety, and promotes and supports measures to improve online safety for Australian-based people,[73] including through statutory powers, educational campaigns and stakeholder collaboration. The eSafety Commissioner's remit is underpinned by four pillars – 'prevention, protection,

---

[69] Anastasia Powell, Nicola Henry, Adrian Scott and Asher Flynn, *Image-Based Sexual Abuse: An International Study of Victims and Perpetrators. Summary Repor*t (February 2020) 12.

[70] The Australian Communications and Media Authority (ACMA) is an Australian Government statutory authority within the Communications portfolio. ACMA was formed on 1 July 2005 with the merger of the Australian Broadcasting Authority and the Australian Communications Authority. ACMA is a 'converged' regulator, created to oversee the convergence of the four 'worlds' of telecommunications, broadcasting, radio communications and the internet. ACMA has responsibilities under four principal Acts – the Broadcasting Services Act 1992, the Telecommunications Act 1997, the Telecommunications (Consumer Protection and Service Standards) Act 1999 and the Radiocommunications Act 1992. See Australian Communications and Media Authority, 'Who We Are' < https://www.acma.gov.au/who-we-are > accessed 4 July 2020; Section 67 of the Enhancing Online Safety Act 2015 requires the ACMA to assist the eSafety Commissioner to perform his/her functions. Section 67 states: '(1) The ACMA must: (a) assist the Commissioner to perform his or her functions and exercise his or her powers; and (b) do so to such extent as the Commissioner reasonably requires. (2) The assistance may include the following: (a) the provision of advice; (b) the making available of resources and facilities. (3) The ACMA must: (a) make available members of the staff of the ACMA to assist the Commissioner to perform his or her functions and exercise his or her powers; and (b) do so to such extent as the Commissioner reasonably requires. (4) The Minister may, by legislative instrument, give directions to the ACMA in relation to the performance of its functions, or the exercise of its powers, under this section. (5) The ACMA must comply with a direction under subsection (4). (6) For the purposes of this section, if a person is an officer or employee whose services are made available to the ACMA under paragraph 55(1)(a) of the *Australian Communications and Media Authority Act 2005*, the person is taken to be a member of the staff of the ACMA. However, the eSafety Commissioner remains separate to the ACMA and does not have to follow any direction of the ACMA. Section 68 of the Enhancing Online Safety Act 2015 states: 'To avoid doubt, the Commissioner is not subject to direction by: (a) the ACMA; or (b) a member or associate member of the ACMA; or (c) a member of the staff of the ACMA; in relation to the performance of a function, or the exercise of a power, by the Commissioner.

[71] Office of the eSafety Commissioner, 'Submission: Review of the Enhancing Online Safety Act 2015 and the Online Content Scheme' (2018) 4.

[72]Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2016/17, 3.

[73] '**Australians** means individuals who are ordinarily resident in Australia'. Enhancing Online Safety Act 2015 Part 1 s 4.

partnerships, and promotion'.[74] The OESC has seen significant development since its initial incarnation as the Office of the Children's eSafety Commissioner. It has evolved from a body supporting children living in Australia to a body designed to protect all individuals who are ordinarily resident in Australia. The powers of the body have been significantly strengthened in the interim.

2.3.2 Online Safety Support before the Children's eSafety Commissioner/eSafety Commissioner

Prior to the establishment of the Office of the Children's eSafety Commissioner, the ACMA (formerly known as the Australian Broadcasting Authority and the Australian Communications Authority before 2005), was the main body tasked with providing regulatory, educational, and awareness-based support for online safety. However other governmental and non-governmental initiatives also existed. These included, for example, the 'ThinkUKnow' governmental cyber safety program, delivering awareness-raising sessions on issues including cyber bullying, sexting and online grooming. Another example includes the Alannah and Madeline Foundation eSmart Schools and eSmart Libraries programs.[75] In Australia, the principal legislation governing internet content was the Broadcasting Services Act 1992. Originally enacted to manage issues such as television broadcasting and license conditions, the Act was expanded in 1999 under the Broadcasting Services Amendment (Online Services) Act 1999 to expand the functions of the Australian Broadcasting Authority to include the regulation of online content. The 1999 amendments to the Broadcasting Services Act 1992 extended the powers of the Australian Broadcasting Authority (now known as the ACMA) 'to oversee the transmission and hosting of internet content in Australia'.[76] The legislation followed the framework outlined by the Federal Government in 1997 which articulated principles by which online content should be regulated and was designed in response to a perception that the community, and particularly, Australian children, needed protection from content which was likely to harm them.[77] The expanded powers included

[74] Office of the eSafety Commissioner, 'Submission: Review of the Enhancing Online Safety Act 2015 and the Online Content Scheme' (2018) 4.
[75] Parliament of Australia, 'Chapter 2 Key issues' <https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Former_Committees/cybersafety/cybersafety/report/c02> accessed 4 June 2020.
[76] The Broadcasting Services Amendment (Online Services) Act 1999.
[77] Peter Coroneos, 'Internet Content Policy and Regulation in Australia' in Kate Crawford and Catherine Lumby (eds), *The Adaptive Moment: A Fresh Approach to Convergent Media in Australia* (University of New South Wales 2011) 53–57; Timothy Hughes, 'Regulation of the Net' (1997) 71 The IT Age: law and information technology 23.

a complaints-based mechanism for content assessment known as the Online Content Scheme.[78] This scheme commenced operation on the 1st of January 2000. As set out in Section 3 of the Broadcasting Services Act 1992, the Online Content Scheme aims to 'provide a means for addressing complaints about certain Internet content',[79] 'restrict access to certain Internet content that is likely to cause offence to a reasonable adult',[80] and 'protect children from exposure to Internet content that is unsuitable for children'.[81] The ACMA operated the reporting mechanism for Australians to complain about offensive and illegal online content. It investigated reports of 'prohibited or potential prohibited' content.[82] Prohibited or potential prohibited content was (and still is) categorised into four areas as per the classification guidelines.[83] These include child sexual abuse content, content advocating terrorism, instruction, incitement or promotion of crime or violence content, and sexually explicit content.[84] While not designed to directly target IBSA, it was the first mechanism developed with the potential to assist in the removal of certain cases of IBSA. This framework operated (and still operates) as a co-regulatory system that is supported by industry codes. Under these industry codes, commercial content providers and certain mobile content services assess some content in advance of uploading, and assess uploaded content in response to complaints, and then apply the appropriate measures to manage end-users access, which may involve take-down, blocking technology to prevent distribution, or access controls, such as restricted access systems like PINs and credit card age verification. The codes also require industry to respond to notices and help parents monitor the online activities of their children and filter unwanted content. The ACMA's responsibilities under the scheme included the investigation of complaints made under schedules 5 and 7 of the Broadcasting Services Act.[85]

---

[78] The Online Content Scheme was established under schedule 5 of the Broadcasting Services Act 1992.
[79] Broadcasting Services Act 1992, s 3(k).
[80] ibid s 3(l).
[81] ibid s 3(m).
[82] Office of the eSafety Commissioner, 'Submission: Review of the Enhancing Online Safety Act 2015 and the Online Content Scheme' (2018) 8.
[83] Broadcasting Services Act 1992, Schedule 7 Part 2 Division, s 20.
[84] Prohibited or potentially prohibited content is content that may be: Refused Classification, or RC, under the National Classification Code, which includes: – illegal material such as child sexual abuse material; – extremely violent and disturbing pornography; – extremist propaganda, incitement to terrorism; and – games that victimise and abuse children or encourage illegal activity; and › X18+ content that contains real depictions of actual sexual activity between consenting adults without violence, coercion or other types of abuse. The online content scheme also seeks to restrict access by children to content that may be suitable for adults, but not children, including: › R18+ content which may for example contain violence, drug use, nudity or realistically simulated sex; and › MA15+ content on certain mobile premium services, or that is commercially provided (other than text and/or still images).
[85] Broadcasting Services Act 1992, Schedules 5 & 7; Optional end-user filters are computer programs designed to limit access to certain types of content on the internet. Users can choose whether or not to install

The ACMA also provided support for online issues through its Cybersmart programme and Digital Citizens Guides. Launched in July 2009, Cybersmart was a national online safety education programme managed by the ACMA as part of the Australian Government's commitment to online safety.[86] The program was specifically designed to meet the needs of children, young people, parents, and teachers and had the primary goal of raising awareness and providing education.[87] The programme aimed to develop 'digital citizens who are able to derive the benefits of online participation while taking responsibility for self-protection by understanding the potential consequences of online behaviour'.[88] This initiative was one of the first in Australia to provide awareness and education on online safety issues. The ACMA Digital Citizens Guides (released in 2009 and updated in 2013) also promoted online safety. The ACMA Digital Citizen Guide of 2009 emphasised safe and secure participation online via three pillars: 'digital etiquette', 'digital literacy', and 'digital security'. The 2013 ACMA Digital Citizens guide promoted 'positive engagement' online alongside 'being cybersmart'. The functions, principles, and aims of the ACMA's initiatives are mirrored in some of the eSafety Commissioner's current functions and educational/awareness campaigns.

2.3.3 Development of the concept of an eSafety Commissioner

The concept of an independent body specifically tasked with supporting and promoting online safety was first proposed in June 2011 by the Australian Parliament's Joint Select Committee (JSC) on Cyber-Safety.[89] The JSC conducted an inquiry into issues around online safety and young people and examined 'the merit of establishing an Online

filters, and if and when to activate them. The eSafety Commissioner and Communications Alliance recognises that some families find filters a useful addition to direct parental supervision, and for that reason supports the availability of end user filters. As there are many filters available, Communications Alliance, supported by the eSafety Commissioner offers a 'Family Friendly Filter program'. This program helps families find a suitable filter to purchase. In order for a filter to be supported and recommended by Communications Alliance it must undergo certain testing and ensure that it prohibits all websites identified by the eSafety Commissioner as harmful. All URLs identified under the Online Content Scheme as harmful are added to a 'prohibited URL filter list 'See Communications Alliance, 'Family Friendly Filters' < https://www.commsalliance.com.au/Activities/ispi/fff > accessed 6 Jan 2021.

[86] As part of the Governments Cyber-Safety Plan, the Government announced funding in the 2008– 2009 Budget of $14.2 million over four years for the ACMA's cyber safety activities. Australian Communications and Media Authority, Annual Report 2008/09.

[87] Australian Communications and Media Authority, Parents' Guide to Online Safety <https://www.ideas.org.au/uploads/events/333/Parenting%20online.pdf> accessed 11 July 2020.

[88] Australian Communications and Media Authority, Annual Report 2009/10.

[89] Australian Parliament Joint Select Committee on Cyber-safety, *High-wire act: Cyber-safety and the young, interim report* (Canberra, Australia: Commonwealth of Australia 2011 — 146)

Ombudsman to investigate, advocate and act on cyber-safety issues'.[90] The inquiry was informed by submissions made by stakeholders. The JSC ultimately did not recommend that such an office should be established. One criticism was that the appointment of an 'Ombudsman' was deemed inappropriate.[91] The Australian and New Zealand Ombudsman Association (the Association) called for 'stronger controls on the use of the term ombudsman'.[92] The Association described the term 'ombudsman' as being 'an independent office, which primarily has a complaint handling and investigation function'. The Association stressed that in situations where the office of an ombudsman is 'under the direction or control of an industry or a government minister, they are not independent'.[93] The report highlighted that using the term ombudsman to describe an office with 'regulatory, disciplinary and/or prosecutorial functions' confuses the role of ombudsman with that of a regulatory body.[94] Another criticism was that the proposed Online Ombudsman was said to overlap with functions already provided by other agencies.[95] Telstra Corporation stated that 'the appointment of a separate Online Ombudsman is not required but such a function could be co-ordinated by the Australian Communications and Media Authority within the existing Australian legislative framework'.[96] Similarly, the Australian Library and Information Association stated that the ACMA 'is already fulfilling the functions of an ombudsman such as investigating, advocating and acting on cybersafety issues'.[97] The Australian Federal Police (AFP) also did not see a need for an additional 'reporting point or investigative structure dedicated solely to cyber safety' as they already provide these functions. Rather the AFP highlighted the need to 'consider an enhanced coordination, longer term evaluation and policy synergies of existing or proposed cyber safety programs'.[98] Yahoo stated that an

---

[90] ibid Terms of Reference clause (a)(viii), 23.

[91] Australian Parliament Joint Select Committee on Cyber-safety, *High-wire act: Cyber-safety and the young, interim report* (Canberra, Australia: Commonwealth of Australia 2011 — 146) 356-357.

[92] Australian and New Zealand Ombudsman Association, Media Release, 18 May 2010, Peak body seeks to halt the misuse of the term Ombudsman, 1.

[93] Australian and New Zealand Ombudsman Association, 'Peak body seeks to halt the misuse of the term Ombudsman' (*Media Release*, 18 May 2010).

[94] Australian Parliament Joint Select Committee on Cyber-safety, *High-wire act: Cyber-safety and the young, interim report* (Canberra, Australia: Commonwealth of Australia 2011 — 146) 356-357.

[95] ibid 364, 367, 368.

[96] Australian Parliament Joint Select Committee on Cyber-safety, *High-wire act: Cyber-safety and the young, interim report* (Canberra, Australia: Commonwealth of Australia 2011 — 146) 364 para 3.28. See Telstra, submission 14, 2-4.

[97] Australian Parliament Joint Select Committee on Cyber-safety, *High-wire act: Cyber-safety and the young, interim report* (Canberra, Australia: Commonwealth of Australia 2011 — 146) 364 para 3.29. See Australian Library and Information Association, submission 16, 13.

[98] Australian Parliament Joint Select Committee on Cyber-safety, *High-wire act: Cyber-safety and the young, interim report* (Canberra, Australia: Commonwealth of Australia 2011 — 146) 365 para 13.30. See Australian Federal Police, submission 64, 25. The AFP submission did not specify which programmes they

'Ombudsman may be duplicative and ignorant of relationships and processes that are already in place' . . . and that they would 'would rather see the investment that would be required to establish an Online Ombudsman's office used to supplement funding to existing organizations that are doing very important work in this area such as law enforcement agencies and the ACMA'.[99] The establishment of such a body was also criticised on the grounds that would lack power over websites hosted outside of Australia, potentially rendering it ineffective.[100] The ACT Council of P & C Associations stated that it believed it would be very difficult for an ombudsman to 'have any power to control what is posted on websites, particularly if hosted overseas'.[101] Similarly, the Internet Industry Association argued that the due to the lack of power over other jurisdictions, an ombudsman may only offer 'symbolic assurance'.[102]

In 2012, the then Federal opposition parties – including the Liberal Party of Australia and the National Party of Australia (known as the Liberal-National Coalition)[103] – conducted

---

are referring to however programmes which they provide or are a partner to include ThinkUKnow, the Cyber Safety Pasifika Program and the Cyber Cooperation Program; ThinkUKnow is an online safety programme delivering interactive training to parents, carers, and teachers through primary and secondary schools across Australia using a network of accredited trainers. Trained AFP and Microsoft volunteers deliver the presentations. See ThinkUKnow < https://www.afp.gov.au/what-we-do/crime-types/child-protection/thinkuknow> accessed 24 February 2022; The Cyber Safety Pasifika Program is delivered by the AFP and the National Rugby League. The programme is aimed at increasing the cyber safety awareness of vulnerable communities in the Pacific region. See Cyber Safety Pasifika < https://www.cybersafetypasifika.org/our-work/latest-news/launch-new-cyber-safety-pasifika-program > accessed 24 February 2022; The Cyber Cooperation Program aims to improve cyber resilience across the Indo-Pacific region. The AFP is a partner to this programme. See Cyber Cooperation Program < https://www.dfat.gov.au/international-relations/themes/cyber-affairs/cyber-cooperation-program/Pages/cyber-cooperation-program > accessed 24 February 2022.

[99] Australian Parliament Joint Select Committee on Cyber-safety, *High-wire act: Cyber-safety and the young, interim report* (Canberra, Australia: Commonwealth of Australia 2011 — 146) 363 para 3.27. See Yahoo!7, submission 2.1, 1.

[100] Australian Parliament Joint Select Committee on Cyber-safety, *High-wire act: Cyber-safety and the young, interim report* (Canberra, Australia: Commonwealth of Australia 2011 — 146) 362-363.

[101] Australian Parliament Joint Select Committee on Cyber-safety, *High-wire act: Cyber-safety and the young, interim report* (Canberra, Australia: Commonwealth of Australia 2011 — 146) 362-363. See ACT Council of P&C Associations Inc, submission 41, 12.

[102]Australian Parliament Joint Select Committee on Cyber-safety, *High-wire act: Cyber-safety and the young, interim report* (Canberra, Australia: Commonwealth of Australia 2011 — 146) 366. See Internet Industry Association, submission 88, 10.

[103] There are three main parties represented in the House of Representatives—the Australian Labour Party, the Liberal Party of Australia, and the Nationals. The Labour Party was formed in 1901. The Liberal Party was formed in 1944. The Country Party was formed in 1920, which was renamed the National Country Party in 1975, the National Party of Australia in 1982, and since 2003 has been known as the Nationals. Since the general election of 1949, the Liberal Party and the Nationals when forming government have done so as a coalition. A merger of the Liberals and Nationals has been suggested on a number of occasions but has never been carried out. However, in 2008 the Queensland branches of the Liberal Party and the Nationals merged to form the Liberal National Party of Queensland. Members of the Liberal National Party of Queensland elected to the Federal Parliament have continued to sit as Liberals or Nationals. See Parliament of Australia, 'Infosheet 22 - Political parties'
<
https://www.aph.gov.au/About_Parliament/House_of_Representatives/Powers_practice_and_procedure/00_-_Infosheets/Infosheet_22_-_Political_parties> accessed 15 July 2020.

an examination into the online safety of children and adolescents.[104] Results from this examination were released in a discussion paper that recommended the establishment of a Children's Online Safety Commissioner. This discussion paper was informed by submissions made by families, schools, individuals, social media experts, and internet service providers. The submissions highlighted that parents and schools felt ill-equipped to deal with the challenge of protecting children from online dangers. In response to this and as part of an election campaign in 2013, the Liberal-National Coalition released the 'Coalitions Policy to Enhance Online Safety for Children'. In this report the parties committed to establishing a Children's eSafety Commissioner to take a 'national leadership role in online safety for children', 'ensure the provision of an effective complaints system', and 'examine existing Commonwealth legislation to determine whether to create a new, simplified cyberbullying offence' [105] if elected. The Liberal-National Coalition formed a Government in September 2013.[106] In January 2014, the Government released a discussion paper seeking submissions in response to its proposed Children's eSafety Commissioner.[107] The paper set out the functions of the proposed Children's eSafety Commissioner which were influenced by New Zealand's Harmful Communications Bill 2013[108] and a report from the Law Reform Committee on its inquiry into sexting.[109]

Figure 3 provides a graphical representation of the development of the OESC from January 2000 to January 2014 as discussed above.

---

[104] The Coalition's Discussion Paper on Enhancing Online Safety for Children (November 2012).
[105] The Coalition's Policy to Enhance Online Safety for Children (September 2013).
[106] The Coalition has been in Government since 2013 and was re-elected again in 2019.
[107] Australian Government Department of Communications, Enhancing Online Safety for Children Public consultation on key election commitments (January 2014).
[108] Harmful Digital Communications Bill, 2013. New Zealand's bill provided for a civil enforcement regime. Under the New Zealand regime, a person complaining of being the subject of a harmful digital communication may make a complaint to the 'Approved Agency'. Under the New Zealand regime, the Approved Agency could, receive and assess complaints about harm caused to persons by digital communications; use negotiation, mediation, and persuasion (as appropriate) to resolve complaints; and investigate complaints.
[109] Law Reform Committee, Parliament of Victory, 'Inquiry into Sexting' *Report of the Law Reform Committee for the Inquiry into Sexting* (Parliamentary Paper No. 230, Session 2010-2013) 'Recommendation 13: That the Victorian Government consider creating a Digital Communications Tribunal, either as a stand-alone body or as a 'list' within the Victorian Civil and Administrative Tribunal, to deal with complaints about harmful digital communications. Development of the Digital Communications Tribunal should be informed by the New Zealand Law Commission's proposal for a Communications Tribunal.' See New Zealand Law Commission, Harmful digital communications: the adequacy of the current sanctions and remedies (Ministerial briefing paper, Wellington 2012) 108.

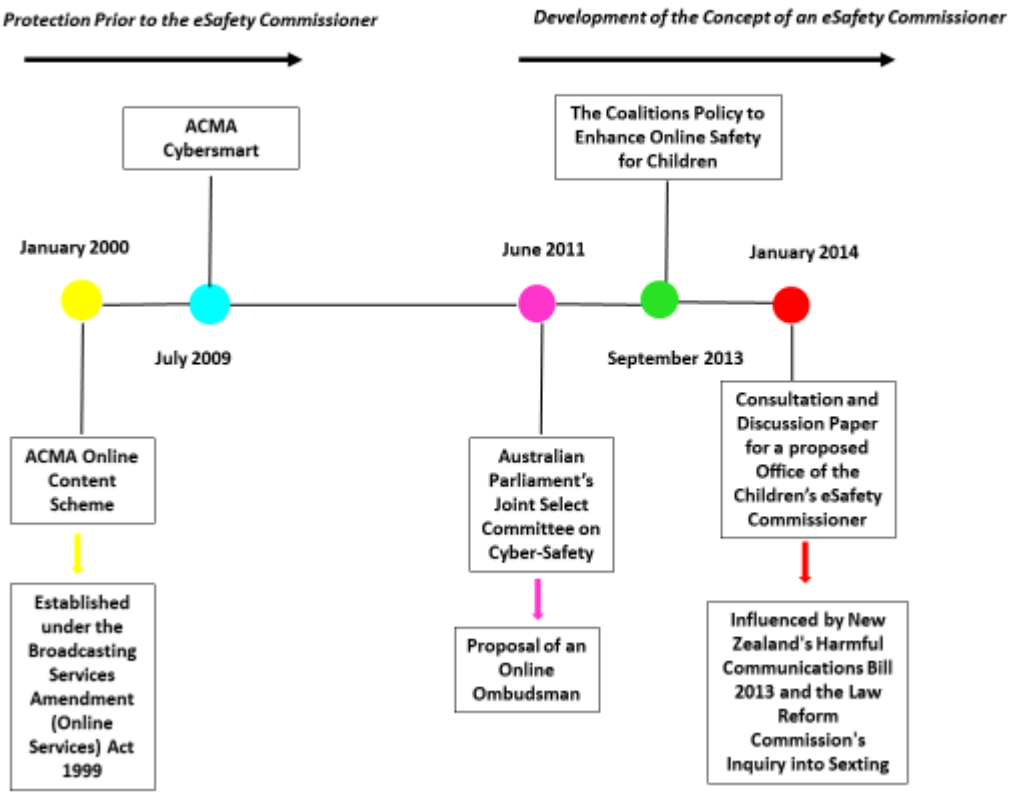


Figure 3 The Development of the OECS from 2000 – 2014

2.3.4 The establishment of the Office of the Children's eSafety Commissioner

On the 1st of July 2015, following commitments made by the Government, the Enhancing Online Safety for Children Act 2015 was enacted. This Act provided the legal basis for the establishment of the Office of the Children's eSafety Commissioner. Alastair MacGibbon (a former Australian Federal Police agent and former Head of Trust and Safety at eBay) was appointed as the first Children's eSafety Commissioner. The Enhancing Online Safety for Children Act 2015 was designed to create a safer online environment for Australian-based children. The key innovation in the legislation was the establishment of a complaints mechanism to be run by the Children's eSafety Commissioner for young Australians experiencing serious cyberbullying.[110] The Children's eSafety Commissioner was also tasked with 'promoting online safety for children', 'coordinating activities of Commonwealth Departments, authorities and

[110] Office of the eSafety Commissioner, 'Submission: Review of the Enhancing Online Safety Act 2015 and the Online Content Scheme' (2018).

agencies relating to online safety for children' and 'administering the online content scheme[111] that was previously administered by the ACMA'.[112]

Cyberbullying complaints scheme

The cyberbullying complaints scheme provides a 'complaints mechanism'[113] for children living in Australia who experience cyberbullying on a 'social media service'.[114] This scheme provides an avenue of redress for young people who have been unsuccessful in resolving their online issue via the social media platform's reporting function.[115] Sections 18 and 19 of the Enhancing Online Safety for Children Act 2015 established this complaints service which allows an Australian based child or someone on behalf of an Australian based child, who has been a target of cyberbullying, to make a complaint to

[111] The online content scheme is separate to the IBSA portal which will be outlined in section 2.3.8.2. The online content scheme allows people to report harmful online content which is prohibited or potentially prohibited to the eSafety Commissioner. The eSafety Commissioner can then investigate whether the content is harmful as per the National Classification scheme which also applies to films, computer games and publications. Before the establishment of the IBSA portal some cases of IBSA could be reported under the Online Content Scheme as sex, sexual activity and nudity are identified as potentially prohibited under the National Classification Scheme. However, the Online Content Scheme does not cover all cases of IBSA. It was not created with IBSA in mind. It has a particular focus on child sexual abuse material. The IBA portal which includes a complaint mechanism was specifically created for IBSA and only deals with the removal of intimate images. Unlike the online content scheme which deals with harmful online content in general, the new scheme is a separate complaints mechanism designed for victims of IBSA.

[112] Enhancing Online Safety for Children Act 2015, s 15.

[113] Office of the eSafety Commissioner, 'Submission: Review of the Enhancing Online Safety Act 2015 and the Online Content Scheme' (2018) 7.

[114] The Enhancing Online Safety Act 2015, s 9 defines a social media service as:
(1) For the purposes of this Act, ***social media service*** means: (a) an electronic service that satisfies the following conditions: (i) the sole or primary purpose of the service is to enable online social interaction between 2 or more end-users; (ii) the service allows end-users to link to, or interact with, some or all of the other end-users; (iii) the service allows end-users to post material on the service; (iv) such other conditions (if any) as are set out in the legislative rules; or (b) an electronic service specified in the legislative rules; but does not include an exempt service (as defined by subsection (4) or (5)). Note: Online social interaction does not include (for example) online business interaction. (2) For the purposes of subparagraph (1)(a)(i), online social interaction includes online interaction that enables end-users to share material for social purposes. Note: Social purposes does not include (for example) business purposes. (3) In determining whether the condition set out in subparagraph (1)(a)(i) is satisfied, disregard any of the following purposes: (a) the provision of advertising material on the service; (b) the generation of revenue from the provision of advertising material on the service. *Exempt services* (4) For the purposes of this section, a service is an ***exempt service*** if: (a) none of the material on the service is accessible to, or delivered to, one or more end-users in Australia; or (b) the service is specified in the legislative rules. (5) If the Commissioner is satisfied that: (a) an electronic service has controls on: (i) who can access material, or who can be delivered material, provided on the service; or (ii) the material that can be posted on the service; and (b) those controls will be effective in achieving the result that none of the material provided on the service could be cyber-bullying material targeted at an Australian child; the Commissioner may, by writing, declare that the service is an ***exempt service*** for the purposes of this section. (6) A declaration made under subsection (5) is not a legislative instrument.

[115] Office of the eSafety Commissioner, 'Submission: Review of the Enhancing Online Safety Act 2015 and the Online Content Scheme' (2018) 7.

the Office of the Children's eSafety Commissioner.[116] The Commissioner has the power to investigate the reported complaints.[117] If the Commissioner finds the material to be cyberbullying material as defined by Section 5 of the Enhancing Online Safety for Children Act 2015,[118] the Commissioner may intervene by issuing a removal notice. If the relevant party does not comply, the Commissioner can issue a civil penalty.

Individuals and social media platforms are compelled to remove cyberbullying material in different manners under the Enhancing Online Safety for Children Act 2015. Different processes apply to social media platforms and individuals. Removal notices for individuals who post cyberbullying material are administered through an end-user notice scheme whereas notices for removal sent to social media services who host cyberbullying material are administered via a 2-tier scheme. As regards actions directed at individuals who post cyberbullying material on social media, such an individual can be issued an end-user notice requiring the person to take all reasonable steps to ensure the removal of the material, refrain from posting any cyber-bullying material for which the child is the target, and/or apologise for posting the material.[119] If an individual fails to comply with an end-user notice, the Commissioner may issue a civil penalty (upon seeking a Court order) forcing the removal of the material by means of an injunction[120] and/or issue a pecuniary penalty.[121]

As regards the hosting of cyberbullying material by online platforms, Part 4 division 2-4 of the Enhancing Online Safety for Children Act 2015 established a two-tiered scheme

---

[116] Enhancing Online Safety for Children Act 2015, s18. Later under Enhancing Online Safety Act 2015, s 18. The complaint is now addressed to the eSafety Commissioner however the process for reporting remains the same.

[117] Enhancing Online Safety for Children Act 2015, s 19. Later under Enhancing Online Safety Act 2015, s 19.

[118] Enhancing Online Safety for Children Act 2015, s 5 – Section 5 states: Cyberbullying material targeted at an Australian child (1) For the purposes of this Act, if material satisfies the following conditions: (a) the material is provided on a social media service or relevant electronic service (b) an ordinary reasonable person would conclude that: (i) it is likely that the material was intended to have an effect on a particular Australian child; and (ii) the material would be likely to have the effect on the Australian child of seriously threatening, seriously intimidating, seriously harassing or seriously humiliating the Australian child; (c) such other conditions (if any) as are set out in the legislative rules; then: (d) the material is cyberbullying material targeted at the Australian child; and (e) the Australian child is the target of the material. (2) An effect mentioned in subsection (1) may be: (a) a direct result of the material being accessed by, or delivered to, the Australian child; or (b) an indirect result of the material being accessed by, or delivered to, one or more other persons. (3) Subsection (1) has effect subject to subsection (4). (4) For the purposes of this Act, if: (a) a person is: (i) in a position of authority over an Australian child; and (ii) an enduser of a social media service or relevant electronic service; and (b) in the lawful exercise of that authority, the person posts material on the service; and (c) the posting of the material is reasonable action taken in a reasonable manner; the material is taken not to be cyberbullying material targeted at the Australian child.

[119] Enhancing Online Safety for Children Act 2015, s 48.

[120] ibid s 48.

[121] Enhancing Online Safety for Children Act 2015, s 46 as informed by Part 4 of the Regulatory Powers (Standard Provisions) Act 2014.

for the 'fast removal'[122] of cyberbullying material from social media services[123] as part of the cyberbullying complaints scheme. The two tiers of the scheme are subject to different levels of regulatory oversight. Any social media service may apply to the Children's eSafety Commissioner to be declared a Tier 1 service under Section 23 of the Act. The application must be made in writing and must demonstrate that the service complies with the basic online safety requirements set out under Section 21 of the Act.[124] If a complaint is made to the Commissioner about cyberbullying material on a Tier 1 service and the material is not removed within 48 hours (or other specified period), the Commissioner may issue the provider with a request to have the cyberbullying material removed from the service.[125] If a Tier 1 service repeatedly fails to comply with requests to remove material over a 12-month period, or the Children's eSafety Commissioner is satisfied that the service does not comply with the basic online safety requirements under Section 21, the Commissioner may revoke the service's Tier 1 status and recommend that the Minister declare the service as a Tier 2 service.[126]

A social media service may be considered as a Tier 2 social media service if the Children's eSafety Commissioner has recommended a Tier 2 status[127] or is a large social media

[122] Enhancing Online Safety for Children Act 2015, Part 4 Division 2-4. Later under The Enhancing Online Safety 2015, Part 4 Division 2-4. See also Office of the eSafety Commissioner, 'Submission: Review of the Enhancing Online Safety Act 2015 and the Online Content Scheme' (2018) 7.

[123] A social media service is defined under section 9 of the Enhancing Online Safety for Children Act 2015 as follows: (1) For the purposes of this Act, ***social media service*** means: (a) an electronic service that satisfies the following conditions: (i) the sole or primary purpose of the service is to enable online social interaction between 2 or more endusers; (ii) the service allows endusers to link to, or interact with, some or all of the other endusers; (iii) the service allows endusers to post material on the service; (iv) such other conditions (if any) as are set out in the legislative rules; or (b) an electronic service specified in the legislative rules; but does not include an exempt service (as defined by subsection (4) or (5)). Note: Online social interaction does not include (for example) online business interaction. (2) For the purposes of subparagraph (1)(a)(i), online social interaction includes online interaction that enables endusers to share material for social purposes. Note: Social purposes does not include (for example) business purposes. (3) In determining whether the condition set out in subparagraph (1)(a)(i) is satisfied, disregard any of the following purposes: (a) the provision of advertising material on the service; (b) the generation of revenue from the provision of advertising material on the service.

[124] Section 21 States: Basic online safety requirements (1) For the purposes of this Act, the ***basic online safety requirements*** for a social media service are as follows: (a) the service's terms of use must contain: (i) a provision that prohibits endusers- from posting cyber-bullying material on the service; or (ii) a provision that may reasonably be regarded as the equivalent of a provision covered by subparagraph (i); (b) the service must have a complaints scheme under which endusers- of the service can request the removal from the service of cyber-bullying material that breaches the service's terms of use; (c) there must be an individual who is: (i) an employee or agent of the provider of the service; and (ii) designated as the service's contact person for the purposes of this Act; (d) the contact details of the contact person must be notified to the Commissioner.

[125] Enhancing Online Safety for Children Act 2015, s 29.

[126] ibid s 25.

[127] As per section 25 a social media service is declared tier 2 if it did not comply to a removal request at the tier 1 level or if it does not comply to the basic online requirements as per section 21.

service.[128] Unlike Tier 1 social media services, if a complaint is made to the Children's eSafety Commissioner about cyberbullying material on a Tier 2 social media service, and the material is not removed within 48 hours, the Commissioner may issue an enforceable social media service notice to remove the material.[129] If a Tier 2 social media service does not comply with a social media service notice, civil penalties may be imposed including a pecuniary penalty[130] or an injunction.[131]

The scheme provides all social media sites with the opportunity to comply with the basic online safety requirements[132] voluntarily under the Tier 1 system, but if the Commissioner decides that a social media service is failing to comply, then that site will be placed under the Tier 2 system and 'coercive regulatory powers' will be used by the Commissioner to assure compliance.[133] According to Berg, the scheme was designed to 'exploit social media sites' need for a strong reputation with consumers in order to facilitate removal in the first instance, and if that fails, the law gives the Children's eSafety Commissioner the power to compel the removal of cyber-bullying material.[134] This scheme therefore allows the Communications Minister to decide when to exercise their enforcement powers.

2.3.5 Expansion of the role of the Office of the Children's eSafety Commissioner

On the 18th of December 2015, the duties of the Office of the Children's eSafety Commissioner expanded to protect persons at risk of family or domestic violence following the signing of the Enhancing Online Safety (Family and Domestic Violence)

[128] A large social media service is defined under section 31(8) as: (8) In determining whether a social media service is a large social media service, the Commissioner must have regard to: (a) if the service has accounts for endusers-: (i) the number of accounts that are held by endusers who are ordinarily resident in Australia; and (ii) the number of accounts that are held by -endusers- who are Australian children; and (b) such other matters (if any) as the Commissioner considers relevant. (9) For the purposes of paragraph (8)(a), the Commissioner may make such assumptions and estimates as the Commissioner considers reasonable.
[129] Enhancing Online Safety for Children Act 2015, s 35.
[130] Enhancing Online Safety for Children Act 2015, s 46 as informed by Part 4 of the Regulatory Powers (Standard Provisions) Act 2014.
[131] Enhancing Online Safety for Children Act 2015, s 48.
[132] ibid s 21.
[133] Chris Berg, 'Submission to the Senate Standing Committee on Environment and Communications Inquiry into Enhancing Online Safety for Children Bill 2014 and the Enhancing Online Safety for Children (Consequential Amendments) Bill 2014' (January 2015).
[134] ibid.

legislative rules 2015.[135] Section 15 of the Enhancing Online Safety for Children Act 2015 conferred three additional functions:

> (1) to promote online safety for persons at risk of family or domestic violence, including on the risks of using technology;
> (2) to support, encourage and conduct educational, promotional, training and community awareness programs that are relevant to online safety for persons at risk of family or domestic violence; and
> (3) to make, on behalf of the Commonwealth, grants of financial assistance in relation to online safety for persons at risk of family or domestic violence [136]

The legislative rules were designed to further protect children under the premise that family or domestic violence facilitated by technology would also inadvertently affect the children in the family.

In response to the expanded functions conferred through the Enhancing Online Safety (Family and Domestic Violence) Legislative Rules 2015, the 'eSafetyWomen' website was launched on the 28th of April 2016. The 'eSafetyWomen' website aims 'to empower women to manage technology risk and abuse and take control of their online experiences'.[137] This is carried out through website features such as a 'personal technology check-up' which tests knowledge of online safety, case study videos of other women's experiences, and a virtual tour of commonly used technologies.[138] In June 2016, the Children's eSafety Commissioner partnered with Women's Services Network to provide workshops to 'frontline and specialist staff, mainstream professionals and those volunteering in the domestic violence field', to provide them with the knowledge to 'support women and families experiencing or recovering from technology-facilitated abuse'.

---

[135] Enhancing Online Safety (Family and Domestic Violence) Legislative Rules 2015. Section 108 of the Enhancing Online Safety for Children Act 2015 provides that the Minister may, by legislative instrument, make legislative rules prescribing matters required or permitted by the Act to be prescribed by legislative rules, or necessary or convenient to be prescribed for carrying out or giving effect to the Act. The Enhancing Online Safety (Family and Domestic Violence) Legislative Rules 2015 is a legislative instrument which confers additional functions upon the Commissioner in relation to the online safety of persons at risk of domestic or familial violence of any kind. Legislative rules are the equivalent to statutory instruments in the Irish context.

[136] Enhancing Online Safety for Children Act 2015, s 15.

[137] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2016/17, 121.

[138] Office of the eSafety Commissioner, 'eSafety Women' < https://www.esafety.gov.au/women > accessed 8 September 2018.

2.3.6 Expansion of the role of the Office of the Children's eSafety Commissioner in relation to IBSA

On the 23rd of May 2017, the duties of the Office of the Children's eSafety Commissioner were further expanded through the Enhancing Online Safety (Intimate Images and Other Measures) Legislative Rules 2017. The purpose of the new legislative rules was to confer additional functions upon the Commissioner in relation to the online safety of Australians (including adults) at risk of having intimate images of them shared without their consent. For the purposes of paragraph 15(1)(r) of the Enhancing Online Safety for Children Act 2015, the following additional seven functions were specified:

> (1) to promote online safety for specified persons;
> (2) to collect, analyse, interpret and disseminate information relating to online safety for specified persons;
> (3) to support, encourage, conduct, accredit and evaluate educational, promotional, training and community awareness programs that are relevant to online safety for specified persons;
> (4) to support, encourage, conduct and evaluate research about online safety for specified persons;
> (5) to publish (whether on the internet or otherwise) reports and papers relating to online safety for specified persons;
> (6) to give the Minister reports about online safety for specified persons;
> (7) to advise the Minister about online safety for specified persons; and
> (8) to consult and cooperate with other persons, organisations, and governments on online safety for specified persons[139]

As an expansion of the scope of the eSafety Commissioner's investigatory or enforcement powers would require primary legislation, the new functions were either educational, advisory, or research in nature. For the purposes of the legislative rules, an 'intimate image' was defined as 'a person engaged in sexual activity; or a person in a manner or context that is sexual; or the genital or anal region of a person or, in the case of a female, the breasts'.[140] A 'specified person' was defined as 'an Australian at risk of having intimate images of them shared without their consent; and an older Australian'.

2.3.7 Further shift from child protection to general protection: From the Children's eSafety Commissioner to the eSafety Commissioner

On the 23rd of June 2017, the Enhancing Online Safety for Children Amendment Act 2017 was enacted. This provided a statutory basis for an expansion in the scope of

[139] Enhancing Online Safety (Intimate Images and Other Measures) Legislative Rules 2017.
[140] ibid s3.

protection provided by the Enhancing Online Safety for Children Act 2015 to protect all residents of Australia regardless of age. Some changes brought under the Act signalled the shift of focus from child protection to general protection. Notably, the title of the 2015 Act was amended to be the Enhancing Online Safety Act 2015[141] and the title of the Children's eSafety Commissioner was changed to be the eSafety Commissioner.[142] Section 15 of the Enhancing Online Safety Act 2015 was updated to reflect this broader remit. Section 15 states:

> (1) The functions of the Commissioner are:
>
> (a) such functions as are conferred on the Commissioner by:
>
> (i) this Act; or
>
> (ii) Schedules 5 and 7 to the *Broadcasting Services Act 1992*; or
>
> (iii) any other law of the Commonwealth; and
>
> (b) to promote online safety for Australians; and
>
> (c) to support and encourage the implementation of measures to improve online safety for Australians; and
>
> (d) to coordinate activities of Commonwealth Departments, authorities and agencies relating to online safety for children; and
>
> (e) to collect, analyse, interpret and disseminate information relating to online safety for Australians; and
>
> (f) to support, encourage, conduct, accredit and evaluate educational, promotional and community awareness programs that are relevant to online safety for Australians; and
>
> (g) to make, on behalf of the Commonwealth, grants of financial assistance in relation to online safety for Australians; and
>
> (h) to support, encourage, conduct and evaluate research about online safety for Australians; and
>
> (i) to publish (whether on the internet or otherwise) reports and papers relating to online safety for Australians; and
>
> (j) to give the Minister reports about online safety for Australians; and
>
> (k) to advise the Minister about online safety for Australians; and
>
> (l) to consult and cooperate with other persons, organisations and governments on online safety for Australians; and
>
> (m) to advise and assist persons in relation to their obligations under this Act; and
>
> (n) to monitor compliance with this Act; and
>
> (o) to promote compliance with this Act; and
>
> (p) to formulate, in writing, guidelines or statements that:
>
> (i) recommend best practices for persons and bodies involved in online safety for Australians; and
>
> (ii) are directed towards facilitating the timely and appropriate resolution of incidents involving cyberbullying material targeted at an Australian child; and

[141] Enhancing Online Safety for Children Amendment Act 2017, s 2.
[142] ibid s 3.

(q) to promote guidelines and statements formulated under paragraph (p); and
(r) such other functions (if any) as are specified in the legislative rules; and
(s) to do anything incidental to or conducive to the performance of any of the above functions.[143]

Section 4 of the 2017 Act amended Section 3 of the 2015 Act (which provides a simplified outline of the Act) requiring the removal of the words '[a] key function of the Commissioner is to administer a complaints system for cyber-bullying material targeted at an Australian child' from the Enhancing Online Safety Act 2015 (formerly known as the Enhancing Online Safety for Children Act 2015). As a substitution, Section 4 of the 2017 Act required the insertion of the words 'The functions of the Commissioner include: (a) promoting online safety for Australians; and (b) administering a complaints system for cyber-bullying material targeted at an Australian child; and (c) coordinating activities of Commonwealth Departments, authorities and agencies relating to online safety for children; and (d) administering the online content scheme under the Broadcasting Services Act 1992.'

The Explanatory Memorandum to the amending legislation noted that the changes would:

> reflect the broader role for online safety that the Commissioner has that goes beyond online safety for Australian children. This broader role includes functions in relation to persons at risk of family or domestic violence, in relation to victims of the non-consensual sharing of intimate images, and in relation to the safe use of the internet by older Australians.[144]

Notably, despite the expanded scope, the 2017 Act did not provide a complaints system for adults but instead merely sought to improve and promote online safety for all Australians through educational initiatives. The 2017 Act confirmed that the eSafety Commissioner would continue to administer the Cyberbullying Complaints Scheme for Australian based children and the Online Content scheme as set out under the Enhancing Online Safety Act 2015.

2.3.8 The Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018

[143] As amended by section 18 and 19 of the Enhancing Online Safety for Children Amendment Act 2017.
[144] Enhancing Online Safety for Children Amendment Bill 2017, Explanatory Memorandum.

The Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018 further expanded the powers of the OESC and for the first time specifically brought IBSA within the scope of the OESC authority. This amending legislation aimed to facilitate the provision of support for victims of IBSA and to provide additional powers to the eSafety Commissioner and an associated framework to enable the removal of intimate images shared without consent from the internet. Crucially, the Act provided the OESC with statutory powers to implement a civil penalty regime to achieve this aim. This legislation will be discussed in greater detail in section 2.3.8.2.

2.3.8.1 What informed the Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018

On the 12th of November 2015, the Government referred the issue of IBSA to the Senate Legal and Constitutional Affairs References Committee (the Committee) for inquiry and report. The Committee's report[145] was published on the 25th of February 2016 and outlined eight recommendations, suggesting that a range of measures be introduced to combat the growing issue of IBSA. The measures recommended included 'criminal and civil law penalties, public education and awareness campaigns, and professional training for police'.[146] However, of particular relevance to this discussion is Recommendation 4, which stated 'the committee recommends that the Commonwealth Government consider empowering a Commonwealth agency to issue take down notices for non-consensually shared intimate images'.[147] This was the first official suggestion of the need for a body with powers to issue take down notices to those hosting intimate images.

On the 28th of October 2016, the Government announced that $4.8 million would be provided to the Children's eSafety Commissioner (now known as the eSafety Commissioner) to develop a national online portal to help counter the effects of IBSA.[148] This funding was part of the $100 million package of the Commonwealth Government to support the implementation of the Third Action Plan of the National Plan to Reduce Violence against Women and their Children.

---

[145] The Senate, Legal and Constitutional Affairs References Committee, *Phenomenon colloquially referred to as 'revenge porn'* (February 2016).
[146] ibid.
[147] ibid.
[148] Mitch Fifield, 'New online reporting tool to tackle non-consensual sharing of intimate images' (Joint Media Release, 28 October 2016) < https://www.mitchfifield.com/2016/10/new-online-reporting-tool-to-tackle-non-consensual-sharing-of-intimate-images/ > accessed 24 February 2022.

Following the provision of funding, on the 23rd of November 2016, the then Minister for Communications (Mitch Fifield) and the Minister for Women (Michaela Cash) announced that the Government would conduct a public consultation process on a proposed civil penalty regime for the non-consensual sharing of intimate images.[149] In May 2017, a discussion paper was published by the Department of Communications and Arts. The discussion paper recommended establishing a prohibition against the sharing of intimate images without consent and the introduction of a civil penalty regime targeted at those involved in the sharing of intimate images, as well as the content hosts.[150] The paper suggested that the eSafety Commissioner would be the most appropriate body to administer this function.[151] The paper suggested that the eSafety Commissioner would already have existing expertise within the Commissioner's Office with regard to online issues.[152] The eSafety Commissioner would have the 'ability to take fast, effective action to have images removed and limiting further distribution with minimal additional stress to victims'.[153] The paper also suggested that there would be a potential reduction of the burden on the criminal justice system by providing a complementary avenue for victims to pursue.[154]

Submissions in response to the discussion paper were made from a range of stakeholders, including women's safety organisations, mental health experts, schools and education departments, victims, and members of the Government's Online Safety Consultative Working Group. The majority of stakeholders were supportive of a civil penalty regime as it would provide victims a timely, accessible, and effective means of redress not available to them through the criminal justice system.[155] Feedback from police submissions indicated that victims are often reluctant to pursue criminal charges against perpetrators, as it could result in lengthy court processes, which can result in amplifying

[149] Naomi Woodley & Josie Taylor, 'Revenge porn civil penalties considered by Government to give victims faster access to justice' (*The World Today*, 23rd November 2016) <https://www.abc.net.au/news/2016-11-23/revenge-porn-civil-penalties-could-serve-quicker-justice/8050054> accessed 17 July 2020.
[150] Australian Government Department of Communications and the Arts, Civil penalties regime for non-consensual sharing of intimate images (Discussion paper, May 2017).
[151] ibid.
[152] ibid.
[153] ibid.
[154] ibid.
[155] Australian Government, Department of Infrastructure, Transport, Regional Development and Communications, 'Civil penalty regime for non-consensual sharing of intimate images' (Submissions) < https://www.infrastructure.gov.au/have-your-say/civil-penalty-regime-non-consensual-sharing-intimate-images > accessed 24 February 2022.

the harm inflicted on the victim. Therefore, a civil penalty regime administered by the eSafety Commissioner was seen as a more appropriate avenue of redress.

On the 16th of October 2017, the eSafety Commissioner launched the pilot image-based abuse portal which provided victims with an avenue to report cases of IBSA, but the OESC had no statutory powers at this stage. This pilot portal was a first step in responding to issues raised by the Senate and Government. The Australian Minister for Communications, Cyber-Safety and the Arts, Paul Fletcher, explained that the pilot image-based abuse portal was designed as a 'test platform to evaluate the volume and complexity of reports' about IBSA.[156]

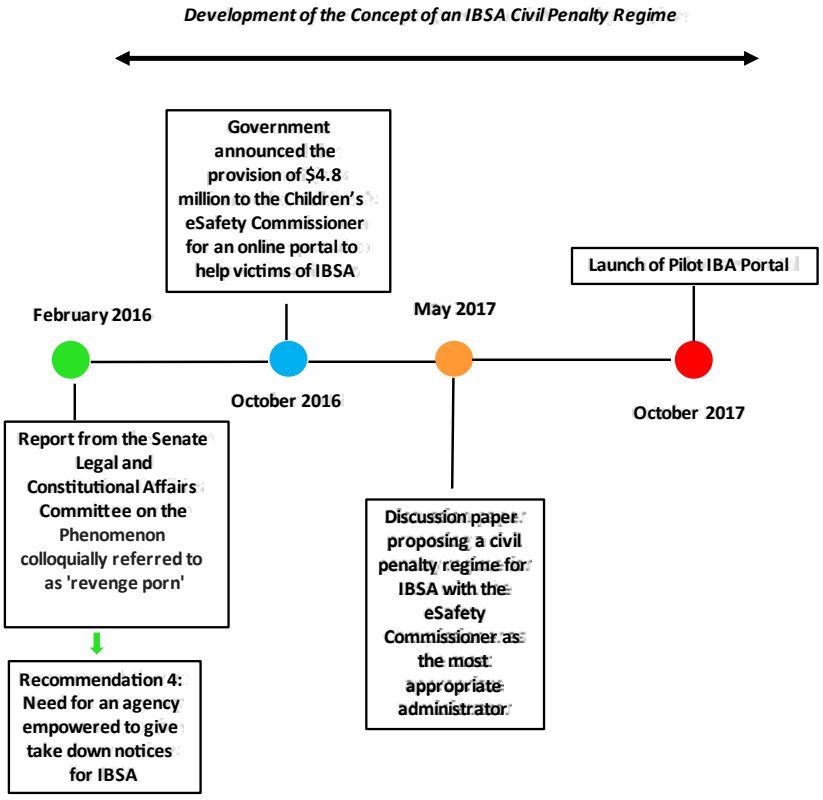


Figure 4 Development of the concept of an IBSA Civil Penalty Regime

2.3.8.2 Overview of the Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018

[156] Paul Fletcher, Minister for Communications, Cyber-Safety and the Arts, Second Reading Speech: Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Bill 2018 <https://www.paulfletcher.com.au/parliamentary-speeches/second-reading-speech-enhancing-online-safety-non-consensual-sharing-of > accessed 12 July 2020.

On the 31st of August 2018 the Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018 was enacted. The Act brought the pilot IBA portal to established status and provided an enforcement dimension to the IBA portal which had previously operated on a voluntary basis without a system for redress. The purpose of this Act was to amend the Enhancing Online Safety Act 2015 and the Broadcasting Services Act 1992[157] to establish a complaints and objections system for the sharing of intimate images without consent.[158] The Enhancing Online Safety (Non-Consensual Sharing of Intimates Images) Act 2018 expanded the eSafety Commissioner's functions to include a complaints and objection system in relation to intimate images posted without consent, powers to issue removal notices to intermediaries and end-users who host a reported intimate image, and power to establish a civil penalty regime. The IBSA scheme applies to social media, relevant electronic and internet services, and end-user perpetrators.[159] The scheme enables the eSafety Commissioner to hold perpetrators accountable through a range of measures, including formal warnings, infringement notices, and the seeking of an injunction or civil penalty order from a court.[160] It offers victims relief by facilitating the rapid removal of intimate images that have been posted online. The Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018 also amended Section 474.17 of the Criminal Code Act 1995 (which criminalises using a carriage service to

[157] Part 13 of the Broadcasting Services Act 1992 governs investigatory processes conducted by the eSafety Commissioner and ACMA. Section 19C of the Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018 which allows for the eSafety Commissioner to conduct investigations into complaints of IBSA is subject to Part 13 of the Broadcasting Services Act 1992. Therefore, the Broadcasting Services Act 1992 is amended to include the Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018 as part of its scope.

[158] Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018.

[159] The Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Act 2018; Lynelle Briggs, *Report of the Statutory Review of the Enhancing Online Safety Act 2015 and the Review of Schedules 5 and 7 to the Broadcasting Services Act 1992 (Online Content Scheme)* October 2018.

[160] The implementation of a civil penalty is governed by the Regulatory Powers (Standard Provisions) Act 2014. Section 82 of the 2014 Act states: 82 Civil penal (1) An authorised applicant may apply to a relevant court for an order that a person, who is alleged to have contravened a civil penalty provision, pay the Commonwealth a pecuniary penalty. (2) The authorised applicant must make the application within 6 years of the alleged contravention. Court may order person to pay pecuniary penalty (3) If the relevant court is satisfied that the person has contravened the civil penalty provision, the court may order the person to pay to the Commonwealth such pecuniary penalty for the contravention as the court determines to be appropriate Note: Subsection (5) sets out the maximum penalty that the court may order the person to pay. (4) An order under subsection (3) is a civil penalty order. Determining pecuniary penalty (5) The pecuniary penalty must not be more than: (a) if the person is a body corporate—5 times the pecuniary penalty specified for the civil penalty provision; and (b) otherwise—the pecuniary penalty specified for the civil penalty provision. (6) In determining the pecuniary penalty, the court must take into account all relevant matters, including: (a) the nature and extent of the contravention; and (b) the nature and extent of any loss or damage suffered because of the contravention; and (c) the circumstances in which the contravention took place; and (d) whether the person has previously been found by a court (including a court in a foreign country) to have engaged in any similar conduct. In this thesis the 'authorised person' is the eSafety Commissioner. The eSafety Commissioner can apply to the federal court for an order to issue a pecuniary penalty for a breach of a specified section of 2018 Act.

harass, menace or cause offence) to include increased penalties for sharing private sexual material in this way.[161] As a result, the Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018 amended Section 474.17 of the Criminal Code Act 1995 to criminalise IBSA as discussed in section 2.2. The explanatory memorandum to the legislation stated that the intent of the Act 'is to send a clear message to the community that the sharing of intimate images without consent is not an acceptable practice'.[162] It intends to 'facilitate the quick removal of images without causing additional distress to the victim'.[163] It also aims to 'complement existing Commonwealth, state and territory criminal laws and the online complaints portal pilot which was launched by the OESC on 16 October 2017'. [164]

The Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Act 2018 sets out the new functions and powers of the eSafety Commissioner in relation to IBSA. Section 44B of the Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Act 2018 prohibits the posting or threat of posting of an intimate image.[165]. Section 44B states:

'(1) A person (the ***first person***) must not post, or make a threat to post, an intimate image of another person (the ***second person***) on:

---

[161] The Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Act 2018 amends s 474.17 of the Criminal Code 1995. Section 474.17 states '(1) A person is guilty of an offence if: (a) the person uses a carriage service; and (b) the person does so in a way (whether by the method of use or the content of a communication, or both) that reasonable persons would regard as being, in all the circumstances, menacing, harassing or offensive.' Now the criminal code (as amended by The Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Act 2018) includes (1) A person commits an offence against this subsection if: (a) the person commits an offence (the ***underlying offence***) against subsection 474.17(1); and (b) the commission of the underlying offence involves the transmission, making available, publication, distribution, advertisement or promotion of material; and (c) the material is private sexual material. The penalty increases from 3 years imprisonment to 5 years imprisonment.

[162] Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Bill 2017, Explanatory Memorandum.

[163] ibid.

[164] ibid.

[165] Mann describes civil penalty provisions as a 'hybrid between the criminal and the civil law'. Gillooley and Wallace-Bruce state that civil penalty provisions 'may be broadly defined as punitive sanctions that are imposed otherwise than through the normal criminal process. These sanctions are often financial in nature, and closely resemble fines and other punishments imposed on criminal offenders. However, the process by which these penalties are imposed is decidedly non-criminal, lacking many of the procedural safeguards built into the criminal process to protect the citizen from arbitrary use of State power.' The Australian Law Reform Committee describe that the 'contravention may be similar to a criminal offence . . . but the procedure by which the offender is sanctioned is based on civil court processes.' Mann explains that these penalties differ from traditional civil remedies in that they do not necessarily bear any 'close relationship to the actual damage caused (that is, they are non-compensatory)'. The Australian Law Reform Committee further explain that civil penalties are not exclusively monetary and may also include 'injunctions, banning orders, licence revocations and orders for reparation and compensation'. See Michael Gillooly & Nii Lante Wallace-Bruce, 'Civil Penalties in Australian Legislation' (1994) 13 University of Tasmania Law Review 269; Kenneth Mann, 'Punitive Civil Sanctions: The Middle ground Between Criminal and Civil Law' (1992) 101(5) Yale Law Journal 1795, 1799, 1815; Australian Law Reform Committee, *Principled Regulation Federal Civil and Administrative Penalties in Australia* (Report 95 — December 2002) para 2.47, 2.51.

(a) a social media service; or
(b) a relevant electronic service; or
(c) a designated internet service;
if:
(d) the first person is ordinarily resident in Australia; or
(e) the second person is ordinarily resident in Australia'[166]

If a person violates Section 44B, the eSafety Commissioner may impose a civil penalty of 500 units.[167] Under Section 19A of the 2018 Act, a person 'depicted'[168] in an intimate image or an 'authorised person'[169] can make a complaint to the OESC if they have 'reason to believe that Section 44B has been contravened in relation to an intimate image of the person.'[170] Furthermore, under Section 19B a person who initially gave consent to the posting of their intimate image but later wishes to retract that consent can make a complaint to object to that image being hosted on a platform. Upon receiving a complaint, the eSafety Commissioner has the power to investigate the complaint under Section 19C of the 2018 Act. After investigating the complaint, and where the eSafety Commissioner is satisfied that the intimate image was posted without consent, the eSafety Commissioner may issue a removal notice for the intimate image. This notice may be issued to a 'social

[166] Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Bill 2018, s 44B.
[167] One unit equals $222 see Notice of Indexation of the Penalty Unit Amount Federal Register of Legislation (Australia) 14 May 2020.
[168] Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Act 2018, s 19A states: *Complaint made by a person depicted in an intimate image* (1) If a person has reason to believe that section 44B has been contravened in relation to an intimate image of the person, the person may make a complaint to the Commissioner about the matter.
[169] Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Act 2018, s 19A states: *Complaint made on behalf of a person depicted in an intimate image* (3) If a person (the ***authorised person***) has reason to believe that section 44B has been contravened in relation to an intimate image of another person (the ***depicted person***), the authorised person may, on behalf of the depicted person, make a complaint to the Commissioner about the matter, so long as: (a) the depicted person has authorised the authorised person to make a complaint about the matter; or (b) both: (i) the depicted person is a child who has not reached 16 years; and (ii) the authorised person is a parent or guardian of the depicted person; or (c) both: (i) the depicted person is in a mental or physical condition (whether temporary or permanent) that makes the depicted person incapable of managing his or her affairs; and (ii) the authorised person is a parent or guardian of the depicted person. (4) The authorised person must make a declaration to the Commissioner to the effect that the authorised person is entitled to make the complaint on behalf of the depicted person.
[170] Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Act 2018, s 19A(1).

media service',[171] 'relevant electronic service'[172] or a 'designated internet service',[173] requiring the provider to remove the image from their platform or service.[174] The eSafety Commissioner may also issue a removal notice to a 'hosting service provider'[175] requiring the provider to cease hosting the image.[176] Furthermore, the eSafety Commissioner may issue a removal notice to an end-user of a social media service, relevant electronic service or designated internet service who posts an intimate image on the service without consent, requiring the end-user to remove the image.[177] If a removal notice is not adhered to, the eSafety Commissioner may issue a civil penalty of 500 penalty units[178] by means of an infringement notice. An infringement notice may also be complemented with an

[171] A social media service is defined under part 1 section 9 of the Enhancing Online Safety Act 2015 as follows: (1) For the purposes of this Act, ***social media service*** means: (a) an electronic service that satisfies the following conditions: (i) the sole or primary purpose of the service is to enable online social interaction between 2 or more endusers-; (ii) the service allows endusers to link to, or interact with, some or all of the other -endusers; (iii) the service allows -endusers to post material on the -service; (iv) such other conditions (if any) as are set out in the legislative rules; or (b) an electronic service specified in the legislative rules; but does not include an exempt service (as defined by subsection (4) or (5)). Note: Online social interaction does not include (for example) online business interaction. (2) For the purposes of subparagraph (1)(a)(i), online social interaction includes online interaction that enables endusers- to share material for social purposes. Note: Social purposes does not include (for example) business purposes. (3) In determining whether the condition set out in subparagraph (1)(a)(i) is satisfied, disregard any of the following purposes: (a) the provision of advertising material on the service; (b) the generation of revenue from the provision of advertising material on the service.

[172] The 2018 Act does not define 'relevant electronic service. An electronic service is defined under part 1 section of the 2015 Act as follows: ***electronic service*** means: (a) a service that allows endusers- to access material using a carriage service; or (b) a service that delivers material to persons having equipment appropriate for receiving that material, where the delivery of the service is by means of a carriage service; but does not include: (c) a broadcasting service (within the meaning of the *Broadcasting Services Act 1992*); or (d) a datacasting service (within the meaning of that Act).

[173] Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Act 2018, s 9A defines Designated internet service as: (1) For the purposes of this Act, designated internet service means: (a) a service that allows end-users to access material using an internet carriage service; or (b) a service that delivers material to persons having equipment appropriate for receiving that material, where the delivery of the service is by means of an internet carriage service; but does not include: (c) a social media service; or (d) a relevant electronic service; or (e) an on-demand program service; or (f) a service specified under subsection (2). (2) The Minister may, by legislative instrument, specify one or more services for the purposes of paragraph (1)(f).

[174] Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Act 2018, s 44D.

[175] Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Act 2018, s 4 states a 'hosting service provider means a person who provides a hosting service'. Section 9C defines a hosting service as: For the purposes of this Act, if: (a) a person (the first person) hosts stored material that has been posted on: (i) a social media service; or (ii) a relevant electronic service; or (iii) a designated internet service; and (b) the first person or another person provides: (i) a social media service; or (ii) a relevant electronic service; or (iii) a designated internet service; on which the hosted material is provided; the hosting of the stored material by the first person is taken to be the provision by the first person of a hosting service.

[176] Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Act 2018, s 44F.

[177] ibid s 44E.

[178] Section 44G States: A person must comply with a requirement under a removal notice to the extent that the person is capable of doing so. Civil Penalty – 500 units. 'Penalty units determine the amount a person is fined when they commit an infringeable offence' See Victoria State Government, 'Penalties and values' <https://www.justice.vic.gov.au/justice-system/fines-and-penalties/penalties-and-values> accessed 24 February 2022. Crimes Act 1914 section 4AA (1) states 'In a law of the Commonwealth or a Territory Ordinance, unless the contrary intention appears: "penalty unit" means the amount of $210 (subject to indexation under subsection (3))'.

enforceable undertaking[179] or an injunction[180] upon the eSafety Commissioner receiving a court order.

An infringement notice[181] is provided for under Section 46A of the Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Act 2018. Under this section, the eSafety Commissioner can issue an infringement notice to a person who posts an intimate image,[182] to a person who does not comply with a removal notice,[183] and to an intermediary who fails to comply with a social media service notice.[184] In order to issue an infringement notice, the eSafety Commissioner does not need to seek a court order,[185] but must satisfy Section 103 of the Regulatory Powers (Standard Provisions) Act 2014.[186] In short, if the eSafety Commissioner issues an infringement notice, the recipient can

[179] 'An enforceable undertaking is a legally binding written agreement in which a person, or organisation, agrees to undertake tasks or actions to rectify, or prevent, a contravention of a law. Entering into an enforceable undertaking is voluntary but is enforceable by a court. It is an administrative alternative to civil or criminal proceedings. Failure to comply with the terms of an enforceable undertaking may result in civil penalties, or court orders such as directions to comply with the undertaking, compensation or other appropriate orders.' See Department of Communications and the Arts, Civil penalties regime for non-consensual sharing of intimate images (Discussion Paper May 2017).

[180] 'An injunction is a court order requiring a person to do, or refrain from doing, a particular action.' See Department of Communications and the Arts, Civil penalties regime for non-consensual sharing of intimate images (Discussion Paper May 2017).

[181] 'An infringement notice is a notice issued by an authority which sets out the particulars of an alleged contravention of an offence or civil penalty provision. An infringement notice can be issued in person or through the post, and will give the person to whom it is issued the opportunity to pay the fine specified in the notice or have the offence heard by a court. Infringement notices are generally issued for minor offences such as failure to respond to a notice or provide information.' See Department of Communications and the Arts, Civil penalties regime for non-consensual sharing of intimate images (Discussion Paper May 2017).

[182] Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Act 2018, s 44B.

[183] ibid s 44G.

[184] ibid s 44k.

[185] Regulatory Powers (Standard Provisions) Act 2014, s 98.

[186] Regulatory Powers (Standard Provisions) Act 2014, s 103 states: 103 When an infringement notice may be given (1) If an infringement officer believes on reasonable grounds that a person has contravened a provision subject to an infringement notice under this Part, the infringement officer may give to the person an infringement notice for the alleged contravention (2) The infringement notice must be given within 12 months after the day on which the contravention is alleged to have taken place. (3) A single infringement notice must relate only to a single contravention of a single provision unless subsection (4) applies. (4) An infringement officer may give a person a single infringement notice relating to multiple contraventions of a single provision if: (a) the provision requires the person to do a thing within a particular period or before a particular time; and (b) the person fails or refuses to do that thing within that period or before that time; and (c) the failure or refusal occurs on more than 1 day; and (d) each contravention is constituted by the failure or refusal on one of those days.

either pay the required amount as per the notice and if not, court proceedings may be brought against them.[187]

The eSafety Commissioner may also apply to the Federal Court of Australia or the Federal Circuit Court of Australia for an enforceable undertaking[188] for violations of Section 44B,[189] Section 44G,[190] and Section 44K[191] of the 2018 Act.[192] Section 115(2) of the Regulatory Powers (Standard Provisions) Act 2014 sets out the different types of enforceable undertakings available as follows:

> (2) If the relevant court is satisfied that the person has breached the undertaking, the court may make any or all of the following orders:
>
> (a) an order directing the person to comply with the undertaking;
>
> (b) an order directing the person to pay to the Commonwealth an amount up to the amount of any financial benefit that the person has obtained directly or indirectly and that is reasonably attributable to the breach;
>
> (c) any order that the court considers appropriate directing the person to compensate any other person who has suffered loss or damage as a result of the breach;
>
> (d) any other order that the court considers appropriate.[193]

Finally, the eSafety Commissioner may apply for an injunction under Section 48 of the 2015 Act[194] when an individual or intermediary fails to comply with a removal notice to

---

[187] Section 46 A of the 2018 Act explains that an infringement notice is governed by Part 5 Division 1 of the Regulatory Powers (Standard Provisions) Act 2014. Section 98 of Part 5 division 1 provides an outline of this part and states: A person can be given an infringement notice in relation to a contravention of a provision that is subject to an infringement notice under this Part. The provision may be a strict liability offence or a civil penalty provision, or both. A person who is given an infringement notice can choose to pay an amount as an alternative to having court proceedings brought against the person for a contravention of a provision subject to an infringement notice under this Part. If the person does not choose to pay the amount, proceedings can be brought against the person in relation to the contravention.

[188] Enhancing Online Safety Act 2015, s 47(3). 'An enforceable undertaking is a legally binding written agreement in which a person, or organisation, agrees to undertake tasks or actions to rectify, or prevent, a contravention of a law. Entering into an enforceable undertaking is voluntary but is enforceable by a court. It is an administrative alternative to civil or criminal proceedings. Failure to comply with the terms of an enforceable undertaking may result in civil penalties, or court orders such as directions to comply with the undertaking, compensation or other appropriate orders.' See Department of Communications and the Arts, Civil penalties regime for non-consensual sharing of intimate images (Discussion Paper May 2017).

[189] Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Act 2018, s 44B (posting of an intimate image).

[190] Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Act 2018, s 44G (non-compliance with a removal notice).

[191] Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Act 2018, s 44k (non-compliance with a social media service notice).

[192] Section 47 of the 2015 Act governs enforceable provisions. The 2018 Act amends section 47, to not only allow the eSafety Commissioner to seek a court order for an enforceable undertaking for violations of section 36 (non-compliance with a social media service notice for the removal of cyberbullying material) of the 2015 Act, but also section 44B, section 44G, and section 44K of the 2018 Act.

[193] Regulatory Powers (Standard Provisions) Act 2014, s 115(2).

[194] Enhancing Online Safety Act 2015, s 48.

remove an intimate image.[195] The operation and effectiveness of these extensive and novel powers as established in the Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018 are explored in Section 4.4[196] Before assessing the OESC powers (as were in place at the time the interviews were conducted) in the context of IBSA, it is first necessary to briefly outline another expansion of the powers of the OESC which occurred in response to a tragic incident.

2.3.9 The Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019

On the 15th of March 2019, an Australian gunman killed 51 people and injured 50 others in a terrorist attack on two mosques in Christchurch, New Zealand. The gunman live-streamed the first 17 minutes of the attack. The gunman also posted a 'manifesto' online, expressing hate speech and white supremacist rhetoric.[197] The video and manifesto went viral and rapidly spread across various social media platforms.[198] On the 6th of April 2019 the Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019 was enacted in response to this event. This Act amends the Criminal Code Act 1995. This amendment further expanded the OESC powers.

Sections 474.35 and 474.36 of the 2019 Act allows the eSafety Commissioner to issue an Abhorrent Violent Material notice to a 'content service'[199] or a 'hosting service'[200] if they

---

[195] Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Act 2018 updated s 48 of the 2015 Act to include s 43 (non-compliance with an end-user notice), s 44B (posting of an intimate image), s 44G (non-compliance with a removal notice), and s 44k (non-compliance with a social media service notice). Section 121 of the Regulatory Powers (Standard Provisions) Act 2014 provides for the various injunctive remedies available to the Court. The Court may issue a restraining injunction (e.g. the Court may issue a restraining injunction in cases whereby a person has threatened to post an intimate image and the Court restrains that posting by issuing an injunction) or a performance injunction (e.g. where someone has posted an intimate image and refuses to remove the image, the Court may issue a performance notice to force the removal of the image.) Section 122 of the Regulatory Powers (Standard Provisions) Act 2014 also sets out that the Court may impose an interim injunction while deciding on whether to impose an injunction under section 121.

[196] No civil penalties or actions have been imposed yet under the 2018 Act.

[197] BBC News, 'Christchurch Shootings: 49 dead in New Zealand mosque attacks' (15 March 2019) < https://www.bbc.com/news/world-asia-47578798 > accessed 17 October 2020; Calla Wahlquist, 'Christchurch shooting gunman intended to continue attacks, say PM' (*The Guardian*,16 March 2019); Charlotte Graham-McLay, 'Death Toll in New Zealand Mosque Shooting Rises to 51' *New York Times* (New York, 2 May 2019).

[198] Office of the eSafety Commissioner, 'ISP Blocking: facts and falsehoods' (24 March 2020) <https://www.esafety.gov.au/sites/default/files/2020-03/eSafety-ISP-Blocking-factsheet.pdf> accessed 21 July 2020.

[199] Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019, s 474.30 states: content service means: (a) a social media service (within the meaning of the Enhancing Online Safety Act 2015); or (b) a designated internet service (within the meaning of the Enhancing Online Safety Act 2015).

[200] Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019 Section 474.30 states: hosting service has the same meaning as in the Enhancing Online Safety Act 2015. For this purpose, disregard subparagraphs 9C(a)(ii) and (b)(ii) of that Act.

are providing access to Abhorrent Violent Material.[201] Section 474.31 states that abhorrent violent material is audio, visual, or audiovisual material 'that records or streams abhorrent violent conduct engaged in by one or more persons' and 'is material that reasonable persons would regard as being, in all the circumstances, offensive' and is produced by a person or persons who is/are

(i) a person who engaged in the abhorrent violent conduct; or
(ii) a person who conspired to engage in the abhorrent violent conduct; or
(iii) a person who aided, abetted, counselled or procured, or was in any way knowingly concerned in, the abhorrent violent conduct; or
(iv) a person who attempted to engage in the abhorrent violent conduct.[202]

The legislation states that it is immaterial whether the material has been altered or whether the conduct was engaged in within or outside Australia.[203]

Section 474.32 of the Act states that a person engages in ***abhorrent violent conduct*** if the person:

(a) engages in a terrorist act; or
(b) murders another person; or
(c) attempts to murder another person; or
(d) tortures another person; or
(e) rapes another person; or
(f) kidnaps another person.

Failure by a content service or hosting service to remove access to the material may constitute a criminal offence. Commonwealth law enforcement agencies are responsible

[201] Providing access to abhorrent violent material is prohibited under section 474.34 of the Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019. Section 474.34 states: (1) A person commits an offence if: (a) the person provides a content service; and (b) the content service can be used to access material; and (c the material is abhorrent violent material; and (d) the person does not ensure the expeditious removal of the material from the content service. (2) For the purposes of subsection (1), it is immaterial whether the content service is provided within or outside Australia. (3) Subsection (1) does not apply to material unless the material is reasonably capable of being accessed within Australia. (4) The fault element for paragraphs (1)(b) and (c) is recklessness. *Hosting service* (5) A person commits an offence if: (a) the person provides a hosting service; and (b) material is hosted on the hosting service; and (c) the material is abhorrent violent material; and (d) the person does not expeditiously cease hosting the material. (6) For the purposes of subsection (5), it is immaterial whether the hosting service is provided within or outside Australia. (7) Subsection (5) does not apply to material unless the material is reasonably capable of being accessed within Australia. (8) The fault element for paragraphs (5)(b) and (c) is recklessness. *Penalty for individual* (9) An offence against subsection (1) or (5) committed by an individual is punishable on conviction by imprisonment for a period of not more than 3 years or a fine of not more than 10,000 penalty units, or both. *Penalty for body corporate* (10) An offence against subsection (1) or (5) committed by a body corporate is punishable on conviction by a fine of not more than the greater of the following: (a) 50,000 penalty units; (b) 10% of the annual turnover of the body corporate during the period (the ***turnover period***) of 12 months ending at the end of the month in which the conduct constituting the offence occurred.
[202] Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019, s 474.31
[203] ibid s 474.31

for prosecuting this offence, however any prosecution first requires the consent of the Attorney-General.[204]

2.3.10 Summary of the functions and powers of the eSafety Commissioner from 2015-2021

As outlined above, the powers and functions of the eSafety Commissioner have evolved and developed from its initial inception as the Children's eSafety Commissioner. The current purpose of the eSafety Commissioner 'is to help safeguard Australians at risk from online harms and to promote safer, more positive online experiences'.[205] From 2015-2021 the OESC executed the aim of safeguarding Australians at risk from online harms through three main statutory schemes. The OESC still administers these schemes under the new Online Safety Act 2021 with some amendments and additional features which will be explained in section 2.5. First, the eSafety Commissioner administers a complaints and civil penalty scheme for Australian-based children who have experienced cyberbullying or seriously threatening, intimidating, harassing or humiliating online behaviour as established under the Enhancing Online Safety for Children Act 2015 and amended by the Enhancing Online Safety for Children Amendment Act 2017.

Secondly, the eSafety Commissioner responds to complaints about illegal and harmful content, including child sexual abuse material through its formal investigation and reporting scheme for prohibited and potentially prohibited online content, as well as abhorrent violent material, known as the Online Content Scheme. This scheme was established under the Broadcasting Services Act Amendment (Online Services) Act 1999 and was amended under the Enhancing Online Safety for Children Amendment Act 2017 to come under the scope of the eSafety Commissioner. The eSafety Commissioner can also respond to complaints about abhorrent violent material under the most recent expansion of the eSafety Commissioners functions under the Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act.

Finally, and of most relevance to this thesis, the eSafety Commissioner responds to complaints about IBSA through its IBA portal. The eSafety Commissioner has the power to impose sanctions for non-compliance under its civil penalty regime. This function was established under the Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Act 2018.

---

[204] ibid s 474.42.

[205] Office of the eSafety Commissioner, 'What We Do' < https://www.esafety.gov.au/about-us/what-we-do> accessed 13 January 2022.

The ability to 'promote safe online experiences' is provided for under Section 15 of the Enhancing Online Safety Act 2015 as amended by the Enhancing Online Safety for Children Act 2017. The eSafety Commissioner promotes safe online experiences by educational resources and training on online safety, developing special initiatives and programmes in response to identified needs (e.g. eSafety Women or IBA portal) and conducting research.

Overall, in order to understand the current aims, functions, and powers of the current eSafety Commissioner, it was important to set out the evolution of the scope of the OESC. The following diagram maps out the development of the OESC from 2015 to 2019:

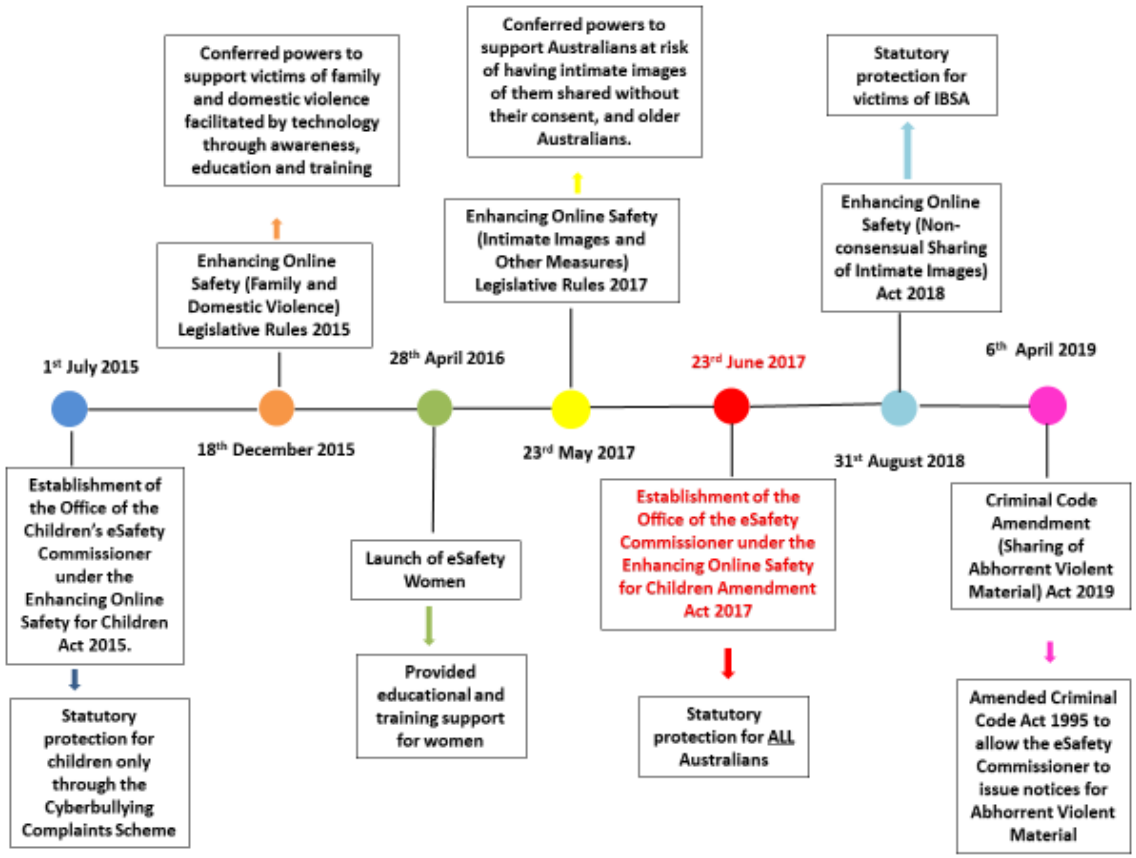


Figure 5 The Development of the OECS from 2015 – 2019

2.4 Preliminary assessment of the design, impact, and operation of the eSafety Commissioner in the context of IBSA

Having set out the functions and powers of the eSafety Commissioner in place at the times the interviews were conducted, this section assesses the effectiveness of the eSafety Commissioner in achieving its aim to 'help safeguard Australians at risk from online

harms and to promote safer, more positive online experiences'[206] in the context of IBSA. A key aim of this thesis is to establish whether Ireland should establish a body influenced by the Australian eSafety Commissioner model as a response to IBSA.[207] In order to inform this analysis, it is first necessary to conduct desk-based research into the effectiveness of the eSafety Commissioner in practice. This assessment provides the starting point for the interviews with experts described in Chapter 3.

Before considering the insights gained from the interviews discussed in Chapter 3, it is necessary to examine some vital secondary sources. The OESC Annual Reports, for example, are a rich source of data for analysis.[208] The eSafety Commissioner is required to publish a report annually on the 'operations' of the eSafety Commissioner during the financial year.[209] The reports include information on the performance of the OESC and provide detail regarding the investigations and assistance provided through the various reporting and removal mechanisms, outreach and awareness programs, research conducted, media engagement and any other projects or collaborative work the eSafety Commissioner has engaged in during the reporting year. In addition, the Government commissioned Briggs report,[210] written in response to the legal requirement to review the operation of the Enhancing Online Safety Act 2015 and the eSafety Commissioner, provides additional insight.[211]

---

[206] Office of the eSafety Commissioner. 'Our Purpose' < https://www.esafety.gov.au/about-us/what-we-do> accessed 4 August 2020.

[207] See discussion of proposed Digital Safety Commissioner and proposed Online Safety Commissioner in Chapter 4 section 4.2.2.2 and section 4.5.

[208] The eSafety Commissioner's annual report is published with the ACMA's annual report. The eSafety Commissioner's funding forms part of the ACMA's appropriation therefore the eSafety Commissioner's financial reporting is included in the ACMA's financial report within their annual report.

[209] Enhancing Online Safety Act 2015, s 66(1) states: 'The Commissioner must, as soon as practicable after the end of each financial year, prepare and give to the Minister, for presentation to the Parliament, a report on the operations of the Commissioner during that year.'

[210] Former Australian Public Service Commissioner, Ms Lynelle Briggs AO, was appointed by the Minister for Communications and the Arts as the independent reviewer.

[211] Enhancing Online Safety Act 2015, s 107. Section 107 states '(1) Within 3 years after the commencement of this section, the Minister must cause to be conducted a review of the following matters: (a) the operation of this Act and the legislative rules; (b) whether this Act or the legislative rules should be amended; (c) whether a delegation should be made under subsection 64(1). The Government set out specific elements to be examined by the Review. These included: 'the extent to which the policy objectives and provisions of the Act remain appropriate for the achievement of the Government's current online safety policy intent; the Commissioner's remit, including roles and responsibilities, and whether the current functions and powers in the Act are sufficient to allow the Commissioner to perform his/her job effectively; whether the current governance structure and support arrangements for the Commissioner provided by the ACMA are fit for purpose; and whether legislative change is required to allow the Commissioner to perform his/her functions and powers more effectively'. See Australian Government Department of Communications and the Arts, 'Review of the Enhancing Online Safety Act 2015 and the Online Content Scheme – discussion' June 2018 4.

These sources – in addition to the expert submissions received in response to the Government review – inform this chapter's initial assessment of the operation of the eSafety Commissioner in the IBSA context. The following section analyses the eSafety Commissioner's educative and awareness-raising functions, the Cyberbullying Complaints Scheme, the Online Content Scheme, and the IBA Portal. However, the core analysis is afforded to the IBA Portal. The other schemes are analysed as they have been in existence for a longer period of time than the IBA scheme and therefore can provide some valuable insight into how the OESC deals with harmful content more generally.

2.4.1 Assessing the effectiveness of the eSafety Commissioner's educative and awareness-raising functions including eSafetyWomen – lessons for IBSA

Before discussing the innovative powers of enforcement entrusted to the eSafety Commissioner, it is first worthwhile to discuss the educational role of the body and soft power it can exercise as a part of that role. The eSafety Commissioner has created many useful resources including the provision of online information, educational tools and programmes for individuals, parents, families, and schools.[212] According to Third, the eSafety Commissioner's website has become a 'focal point for online safety issues.'[213] It is a 'trusted portal' for access to 'high quality' online safety resources.[214] Its role in providing education and awareness is 'critical' to address 'urgent' online issues. In the context of IBSA, the eSafety Commissioner carries out its soft power role through providing education and resources via virtual classrooms, online safety programs, eSafety Women, and frontline worker training. The OESC also exercises its soft power role through raising awareness via the eSafety outreach programs and through media and communications engagement. Furthermore, the eSafety Commissioner fosters key partnerships with stakeholders and encourages collaboration.

Through its educational role, the eSafety Commissioner aims to provide a 'one-stop-shop' for online safety information for all Australians.[215] The eSafety Commissioner recognises that education is an essential part of addressing complex social issues online.[216] The

[212] Australian Government Department of Communications and the Arts, Review of the Enhancing Online Safety Act 2015 and the Online Content Scheme – discussion (June 2018) 4.
[213] Amanda Third, 'Submission to the Review of the Enhancing Online Safety Act 2015 and the Online Content Scheme' (2018) 2.
[214] ibid.
[215] Office of the eSafety Commissioner, 'Submission: Review of the Enhancing Online Safety Act 2015 and the Online Content Scheme' (2018) 120.
[216] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2016/17, 11.

eSafety Outreach programme focuses on providing 'nationally coordinated online safety education' through various platforms and resources.[180] The OESC supports various groups of people including students, teachers, parents, carers, community organisations, law enforcement, and youth workers through education. Information and resources on the eSafety website specifically relating to IBSA include webpages for 'How to report intimate images to eSafety',[217] 'How to remove intimate images',[218] 'how to deal with sexting'[219] and 'how to deal with sextortion'.[220] It also includes fact pages on IBSA statistics and general information on IBSA[221] including information on federal, state and territory laws which can be used to target IBSA.[222] During 2015-2016, the eSafety Commissioner's website received 788,761 visitors, with 2,959,567 pages of content viewed.[223] These figures decreased during 2016-2017 with the website receiving 735,995 visitors, with 2,786,450 pages of content viewed.[224] However, by 2018 the Commissioner's website received a significant increase in engagement with 779,271 visitors and 3,114,717 pages of content viewed.[225] The period of 2018-2019 also saw growth in website engagement, with the website receiving 1,218,407 visitors, with 3,858,791 pages of content viewed.[226] However, the reporting period of 2019-2020 saw the most significant increase in website engagement with over 1.54 million website views and more than 5.48 million page views.[227] The period of 2020-2021 saw a slight decrease in website engagement with 1.4 million visits to the website and 5.37 million page

[217] Office of the eSafety Commissioner, 'How to report IBSA' < https://www.esafety.gov.au/report/image-based-abuse> accessed 15 August 2020.
[218] Office of the eSafety Commissioner, 'Get help to remove images and video' <https://www.esafety.gov.au/key-issues/image-based-abuse/take-action/get-help-remove-images-video> accessed 15 August 2020.
[219] Office of the eSafety Commissioner, 'Sending nudes and sexting' < https://www.esafety.gov.au/key-issues/staying-safe/sending-nudes-sexting> accessed 15 August 2020.
[220] Office of the eSafety Commissioner, 'Deal with sextortion' < https://www.esafety.gov.au/key-issues/image-based-abuse/take-action/deal-with-sextortion> accessed 15 August 2020.
[221] Office of the eSafety Commissioner, 'Impacts and Needs' <https://www.esafety.gov.au/about-us/research/image-based-abuse/impacts-needs> accessed 15 August 2020.
[222] Office of the eSafety Commissioner, 'Deal with sextortion' < https://www.esafety.gov.au/key-issues/image-based-abuse/take-action/deal-with-sextortion> accessed 15 August 2020.
[223] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2015/16, 128.
[224] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2016/17, 122.
[225] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2017/18.
[226] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2018/19, 217.
[227] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2019/20, 202.

views.[228] While the almost consistent continued increase in website engagement would suggest that the eSafety Commissioner's materials and resources are being utilised, it is unknown where this engagement is focused. These figures show a general overview of engagement with the website and the annual reports do not specify the webpages that were viewed. Therefore, it is unclear whether the educational resources for IBSA are reaching IBSA victims or stakeholders. The question of whether victims of IBSA are aware of the OESC and its educational resources is addressed in Chapter 3.

A core educational tool used by the OESC is the Virtual Classroom.[229] Virtual Classrooms and webinars provide opportunities for scalability and reach. In 2015, key topics included cyberbullying, being a good bystander, and the internet and the law.[230] By 2017 more topics were added including 'Respectful Chat', 'Keep it Sweet Online', and 'What's your Brand?'.[231] While these topics are not specific to IBSA, they provide insight into the issue and the information provided can be applied to IBSA and other online harmful behaviours. The presentations are both live and on-demand, with strong interactive elements including live chats.[232] Since the 1st of July 2015, the OESC provided online safety education through Virtual Classrooms to 59,376 students, parents, teachers and community workers over 125 events.[233] During 2016-2017, the number of attendees to the Virtual Classrooms increased to 66,889 attendees over 117 events.[234] The number of attendees also increased in 2017-2018, with 124895 people attending across 78 events.[235] By 2018-2019, this number decreased to 105107 attendees across 39 events.[236] Similarly in 2019-2020, there was a further decrease in the number of attendees to 68,706 across 47 events. A further decrease in Virtual Classroom events was also seen in 2020-2021, with 39 events held. However, the number of attendees increased during this reporting

[228] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2020/21, 204.
[229] Office of the eSafety Commissioner, 'Virtual Classrooms' <https://www.esafety.gov.au/educators/virtual-classrooms > accessed 18 October 2020.
[230] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2015/16.
[231] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2017/18.
[232] Office of the eSafety Commissioner, 'Virtual Classrooms' <https://www.esafety.gov.au/educators/virtual-classrooms > accessed 18 October 2020.
[233] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2015/16, 131
[234] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2016/17, 122.
[235] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2017/18, 130.
[236] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2018/19, 214.

period to 136,488.[237] Considering the size and population of Australia, the number of attendees and Virtual Classroom events can be considered quite low. Furthermore, the figures of the 'number of attendees' provided by the annual reports do not provide a breakdown of the attendees roles or demographics.

The eSafety Commissioner also provides education by connecting people to key organisations who engage with and provide support for online safety issues. Organisations who want to provide support can apply to the eSafety Commissioner who will certify the organisation as a 'certified training provider' upon passing the application screening. On 1 June 2016, the Office launched the 'Find a certified online safety program provider' form, which allowed schools, community groups, sporting groups and others to contact a list of participating programme providers with a single enquiry. This initiative helped the enquirer to quickly and easily find options to help them receive the online safety programme that best fits their needs. In 2016 there were 22 certified training providers.[238] By 2018, the number of providers increased to 36.[239] Out of the 36 certified training providers, 34 offered support for IBSA.[240] The common areas which they provide support for which relate to IBSA are 'sending nudes', 'illegal content', 'harmful content', 'offensive content', 'privacy and personal information', 'sexting', and 'digital reputation'.[241] During 2019-2020, the eSafety Commissioner implemented the Trusted eSafety Providers Program which replaced the Certified Training Providers Scheme. The updated programme builds on the previous model and focuses on ensuring providers meet 'high thresholds for content quality and are up-to-date with the latest online safety trends

[237] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2020/21, 219.
[238] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2015/16, 128.
[239] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2017/18,134; The following is the list of 36 trusted eSafety providers: Alannah & Madeline Foundation, Anglican Schools Commission Southern Queensland, Backflips Against Bullying, Brainstorm Productions Pty Ltd, Bravehearts, Bully Zero, Cyber Safety Project, Cyber Safety Solutions (Susan McLean), Cybersafe Families, Digital Nutrition (Jocelyn Brewer), Elephant Ed, Evolve Education, Eyes Open Social Media Safety, Family Planning Victoria, Inform and Empower, Internet Safe, Education (Brett Lee), Jonny Shannon Pty Ltd, Life Education Australia, Mind Blank Ltd, Online Guardians, PROJECT ROCKIT, Real Talk, Resilience by Design, Roar Educate, Safe on Social Media Pty Ltd (Kirra Pendergast), South Eastern Centre Against Sexual Assault (SECASA), Student Edge, The Carly Ryan Foundation Inc, The Cyber Safety Lady, The Modern Parent, WA Child Safety Services, yourtown (Kids Helpline @ School), Youth Wellbeing Project, ySafe. See Office of the eSafety Commissioner, 'eSafety Trusted Providers' <https://www.esafety.gov.au/educators/trusted-providers/find-providers> accessed 15 August 2020.
[240] Office of the eSafety Commissioner, 'eSafety Trusted Providers' <https://www.esafety.gov.au/educators/trusted-providers/find-providers> accessed 15 August 2020.
[241] ibid.

and research'.[242] 31 providers applied to the program when it launched in December 2019, 28 of whom were endorsed in March 2020.[243] The annual reports do not publish the number of referrals made by the eSafety Commissioner to the trusted eSafety providers and do not provide information regarding the level of collaboration that exists between the eSafety Commissioner and the trusted eSafety Providers. The expert interviews discussed in Chapter 3 address the level of collaboration with the Alannah and Madeline Foundation which is a trusted eSafety provider of the eSafety Commissioner.

eSafetyWomen is a key educational resource provided by the eSafety Commissioner which provides support for victims of IBSA. eSafetyWomen aims 'to empower women to manage technology risk and abuse and take control of their online experiences'.[244] In particular, eSafetyWomen provides support for online abuse which targets women, including IBSA as outlined in section 2.3.5.[245] During 2016-2017, the eSafetyWomen website received 53,281 visitors, with 183,074 pages of content viewed.[265] Popular areas of content included information about dealing with image-based abuse as well as the interactive 'check-up' testing knowledge about online safety and security.[246] During 2017–18, the website received 51,268 unique visits, with 74,448 pages of content viewed.[247] The most popular resources included the technology checkup, 'take the tour' interactives and video case studies.[248] During 2018-2019 there was 23,855 visitors to the eSafetyWomen website, with 99,925 page views. [249] From 2019-2020, there were 35,321 page views with 77,361 pages of content viewed.[250] Popular topics included 'Covid-19: advice for women experiencing domestic violence' and 'International advice for frontline workers supporting women'.[251] The success of eSafetyWomen was recognised in the

[242] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2019/20, 222.
[243] ibid.
[244] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2016/17, 121.
[245] Office of the eSafety Commissioner, 'eSafety Women' < https://www.esafety.gov.au/women > accessed 8 September 2018.
[246] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2016/17, 121.
[247] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2017/18, 132.
[248] ibid.
[249] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2018/19, 215.
[250] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2019/20, 223.
[251] ibid.

United Nations Committee on the Elimination of Discrimination against Women in July 2018.[252]

In June 2016, eSafetyWomen partnered with Women's Services Network to provide workshops to 'frontline and specialist staff, mainstream professionals and those volunteering in the domestic violence field', to provide them with the knowledge to 'support women and families experiencing or recovering from technology-facilitated abuse' including IBSA.[253] A total of 331 participants attended 26 workshops held in centres across five states (Queensland, New South Wales, South Australia, Victoria and Western Australia).[254] The number of participants and workshops increased in 2017 with more than 2,600 participants attending over 150 workshops held across all states and territories.[255] By 2019 the eSafety Commissioner has provided training for over 5500 frontline professionals across every state and territory to help women experiencing technology facilitated abuse.[256] According to the OESC the eSafetyWomen workshops receive positive feedback with 82 per cent of respondents to the post-workshop survey rating the workshops as 'excellent' and 17.5 per cent rating the workshops as 'good' in the surveys given to workshop participants after the completion of their workshop in 2018-2019.[257] The eSafety Commissioner recognised the importance of this training and consequently in 2018 launched eSafetyWomen online training for frontline workers to complement the existing face-to-face eSafetyWomen workshops.[258] In 2019-2020 more than 974 frontline workers registered to undertake this online training. With the heightened risk of family and domestic violence posed by Covid-19 and the health risks, the delivery of face-to-face training formats were adapted to online webinars from April 2020.

However, while the eSafety Commissioner provides many effective educational tools some industry stakeholders have highlighted that many social media services already provide tools and safety protections and the Office should 'support these efforts rather

[252] United Nations Committee, *Eighth Periodic Report on the Elimination of Discrimination against Women* (20 July 2018) 4,5.
[253] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2015/16, 130.
[254] ibid.
[255] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2017/18, 132.
[256] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2018/19, 215.
[257] ibid There was no further information published about these surveys including the number of surveys received.
[258] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2018/19, 215

than compete with them'.[259] Industry representatives from the Digital Industry Group Inc (DIGI)[260] have argued that the Office needs to improve in encouraging greater awareness for existing educational tools and initiatives instead of 'duplicating the significant investment already made by other groups'.[261] Communications Alliance and the Australian Mobile and Telecommunications Association stated that there may be a 'reasonable degree of duplication'.[262]

In order to 'build public confidence and the public profile of online safety issues',[263] the OESC actively engages with the media and audiences through TV, radio, print and social media.[264] The OESC uses these media channels as mechanisms to engage with existing stakeholders and grow audience numbers.[265] Social media platforms are one of the most used mediums for disseminating IBSA. As a result, the OESC currently uses a range of social media channels (including Facebook, Twitter, YouTube, Instagram, Snapchat, and LinkedIn) and posts a mixture of content, including specific announcements like the launch of new resources and initiatives and advice and guidance on specific online safety issues.[266] Cyberzine is the Office's monthly e-newsletter featuring up-to-date resources, information and current advice about online safety including IBSA. In 2016 Cyberzine had 6,724 subscribers, with this number growing by approximately 175 each month.[267] By 2019 Cyberzine had over 26,500 subscribers.[268]

During 2019, the eSafety Commissioner played a key role in the planning and delivery of a national online safety awareness campaign, led by the Department of Communications

[259] Digital Industry Group Inc (DIGI), 'DIGI Submission to the review of the Enhancing Online Safety Act 2015' (August 2018) 4.
[260] DIGI is a not for profit industry association advocating for the digital industry in Australia. Its mission is to 'advocate for policies that enable a growing Australian technology sector that supports businesses and Internet users, in partnership with industry, governments and the community.' Members include Facebook, Twitter, Verizon Media, and Google. See DIGI, 'About DIGI' < https://digi.org.au/about/ > accessed 24 February 2022.
[261] Digital Industry Group Inc (DIGI), 'DIGI Submission to the review of the Enhancing Online Safety Act 2015' (August 2018) 5.
[262] Communications Alliance and the Australian Mobile and Telecommunications Association, 'Submission to the Department of Communications and the Arts Reviews of the Enhancing Online Safety Act 2015 and the Online Content Scheme – discussion paper' (25 July 2018).
[263] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2015/16, 136.
[264] ibid.
[265] ibid.
[266] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2018/19, 217.
[267] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2015/16, 136.
[268] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2018/19, 217.

and the Arts. The campaign 'Start the Chat' was aimed at parents, carers, teachers and others with young people in their lives. It aimed to raise awareness of online safety issues and empower the audience to have 'positive, constructive conversations with their children'.[269] This was the first large-scale campaign associated with the eSafety Commissioner and involved advertisements placed in mainstream media, including online, print, radio and television, as well as outdoor advertising.[270]

While it is clear that the eSafety Commissioner is exercising its educative powers through awareness raising and outreach, it is unclear whether this engagement is having the intended effect of reaching victims of IBSA or potential perpetrators of IBSA. The semi-structured interviews discussed in Chapter 3 examine the eSafety Commissioner's level of visibility to victims of IBSA from a stakeholder's perspective.

Overall, the OESC appears to play an important role in providing educational tools and raising awareness within Australian communities generally, however, the number of cases of IBSA continues to rise. This may be because the OESC is not reaching enough people and therefore victims are not aware of the help available through the OESC. Also, the eSafety Commissioner's initiatives may not be reaching potential perpetrators to show them that IBSA is an offence and that it is not accepted by society. It could also be posited that the growing number of reported cases of IBSA may actually be attributed to a greater awareness for the OESC and IBSA as a result of these initiatives and this has led to greater reporting levels hence an increase in cases.

The OESC website engagement has seen an almost consistent increase from 2015-2021, reaching 1.54 million visitors and 5.48 million page views in one reporting period. However, while these are impressive figures, the OESC annual reports do not specify what content is being viewed and how many visitors are engaging with the IBA portal and associated resources and educational tools. As a result, it is unclear what proportion of visitors engage with the IBA portal page and associated materials. Therefore, the success for the OESC website cannot be translated to a success of the IBA portal specifically and therefore it is unknown how successful the IBA portal actually is in practice in the context of page reviews and visitors. It is important for the OESC to know who they are reaching through their educative functions in the context of IBSA. It is

[269] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2018/19, 217.
[270] ibid.

important that the OESC reach potential victims of IBSA but also potential perpetrators. However, it is clear that the OESC website as a whole is a valuable resource and provides a one stop shop for information and educational tools and resources.

Collaboration is a key focus of the OESC as seen through the Trusted eSafety Providers Program. However, while it is clear that the OESC promote collaboration, to what extent it is utilised is unclear. The annual reports do not publish the number of referrals made by the OESC to the trusted eSafety providers and do not provide information regarding the level of collaboration that exists between the OESC and the trusted eSafety Providers. There should be a requirement to publish this information.

While education and training are vital to ensure that victims and those in positions of support are better informed, and to ensure that potential perpetrators are aware of the harm IBSA, education alone is insufficient. While education and awareness are preventative measures, there is still need for responsive measures. The prevalence of IBSA is yet to abate and as a result the merit of the OESC enforcement responses are considered below.

2.4.2 Assessing the effectiveness of the eSafety Commissioner's Cyberbullying Complaints Scheme – lessons for IBSA

As explained in section 2.3.4, the cyberbullying complaints scheme provides a 'complaints mechanism'[271] for children living in Australia who experience cyberbullying. This scheme allows children and young people to report an issue of online cyberbullying to the eSafety Commissioner who can help in the removal of the cyberbullying material and also help prevent the cyberbullying. This scheme provides an avenue of redress for young people who have been unsuccessful in resolving their online issue via the social media's platform reporting function.[272] The Commissioner has the power to investigate the reported complaints.[273] If the Commissioner finds the material to be cyberbullying material as defined by part 1 Section 5 of the Enhancing Online Safety for Children Act 2015,[274] the Commissioner may intervene by issuing a removal notice. If the relevant

[271] Office of the eSafety Commissioner, 'Submission: Review of the Enhancing Online Safety Act 2015 and the Online Content Scheme' (2018) 7.
[272] ibid.
[273] Enhancing Online Safety for Children Act 2015, s 19. Later under Enhancing Online Safety Act 2015, s 19.
[274] Enhancing Online Safety for Children Act 2015, s 5 – Section 5 states: Cyberbullying material targeted at an Australian child (1) For the purposes of this Act, if material satisfies the following conditions: (a) the material is provided on a social media service or relevant electronic service (b) an ordinary reasonable person would conclude that: (i) it is likely that the material was intended to have an effect on a particular

party does not comply, the Commissioner can issue a civil penalty. As set out in section 2.3.4, this scheme has been in operation since 2015. Consequently, there is a rich source of data available on the functioning of this mechanism. As the IBSA reporting mechanism and civil penalty regime is similar to that of the cyberbullying scheme, lessons learned from the functioning of the cyberbullying scheme provides insight of relevance to the IBSA process.

From the 1st of July 2015 to the 30th of June 2016 the eSafety Commissioner investigated 186 serious cyberbullying complaints.[275] During this period, the eSafety Commissioner's average response time was under 7 hours upon receipt of the complaint.[276] From the 1st of July 2016 to the 30th of June 2017, the eSafety Commissioner investigated 305 complaints about serious cyberbullying.[277] This is an increase of 63% from the previous period. The response time to complaints during this period was less than 3 and a half hours of receipt of the complaint,[278] reducing its response time by 3 and a half hours from the previous period. Between the 1st of July 2017 and the 30th of June 2018, the eSafety Commissioner received 409 complaints, an increase of 34 per cent from 2016–2017.[279] Over 95 per cent of complaints received were 'actioned'[280] within 48 hours and over 75 per cent of complaints were 'finalised'[281] within five working days.[282] Between the 1st of July 2018 and the 30th of June 2019, the eSafety Commissioner received 531 complaints

Australian child; and (ii) the material would be likely to have the effect on the Australian child of seriously threatening, seriously intimidating, seriously harassing or seriously humiliating the Australian child; (c) such other conditions (if any) as are set out in the legislative rules; then: (d) the material is cyberbullying material targeted at the Australian child; and (e) the Australian child is the target of the material. (2) An effect mentioned in subsection (1) may be: (a) a direct result of the material being accessed by, or delivered to, the Australian child; or (b) an indirect result of the material being accessed by, or delivered to, one or more other persons. (3) Subsection (1) has effect subject to subsection (4). (4) For the purposes of this Act, if: (a) a person is: (i) in a position of authority over an Australian child; and (ii) an enduser of a social media service or relevant electronic service; and (b) in the lawful exercise of that authority, the person posts material on the service; and (c) the posting of the material is reasonable action taken in a reasonable manner; the material is taken not to be cyberbullying material targeted at the Australian child.

[275] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2015/16, 122.

[276] ibid.

[277] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2016/17, 115.

[278] ibid.

[279] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2017/18, 124.

[280] In the context of the Annual Reports, 'actioned' typically means when the OESC first starts to investigate/respond to the received complaint.

[281] No definition of this term provided in the report. In this context 'finalised' could mean the close of the investigation or the close of the case.

[282] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2017/18, 124.

about cyberbullying, an increase of 30 per cent from 2017–18.[283] This increase of 30 percent continued in 2019-2020 with the eSafety Commissioner receiving 690 complaints about cyberbullying material.[284] During the reporting period of 2020-2021, the OESC received 934 complaints about cyberbullying, an increase of 35 per cent from the previous reporting period. Unfortunately, the 2018/2019, 2019-2020, and 2020-2021 annual reports released no time frames on how quickly complaints were dealt with or responded to during these reporting periods. Considering the viral nature of the internet, fast removal of harmful material is essential. As a result, understanding the time frames for which the eSafety Commissioner can remove harmful material is important. A question identified as being important to consider during the semi-structured interviews discussed in Chapter 3 is whether the OESC responds to complaints about harmful material such as intimate images in an effective manner considering the time frames of removal.

It is also unreported as to whether cyberbullying material reported to the OESC remains offline permanently (or even for an extended period) or whether victims experience revictimization through the material resurfacing on other platforms by either the original or new perpetrators. Understanding whether the reported material remains offline once reported to the eSafety Commissioner in the context of cyberbullying material would provide a better understanding as to whether victims of IBSA would be able to regain control of their intimate images.

From 2015-2018, the eSafety Commissioner worked collaboratively with 14 social media platforms to remove cyberbullying material.[285] On average, the material was removed in less than a day.[286] The development of key partnerships with social media platforms through the two tiered scheme which forms part of the eSafety Commissioner's response to cyberbullying through the complaints scheme has been described as 'successful'[287] in ensuring the fast removal of cyberbullying material. The success of these collaborative efforts may be mirrored when tackling IBSA, as the eSafety Commissioner has already

[283] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2018/19, 204.

[284] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2019/20, 210.

[285] Office of the eSafety Commissioner, 'Working with social media' < https://www.esafety.gov.au/about-us/consultation-cooperation/working-with-social-media> accessed 16 August 2020. The tier 1 platforms include: airG, ASKfm, Flickr, Roblox, Snapchat, TikTok, Twitter, Yahoo 7 Answers, Yahoo 7 Groups, Yubo, and WeChat. The tier 2 platforms include: Facebook, Instagram, and Youtube.

[286] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2015/16; Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2016/17; Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2017/18.

[287] Department of Home Affairs, 'Reviews of the Enhancing Online Safety Act 2015 and the Online Content Scheme' (August 2018) 6.

established a working relationship with these platforms. Results gathered from the semi-structured interviews establish the level of collaboration between the eSafety Commissioner and key stakeholders from a stakeholder's perspective.

It is also notable that the eSafety Commissioner has not yet needed to issue end-user notices or enforce removal notices as it has built positive relationships with intermediaries to achieve the 'desired outcome' of removing cyberbullying material.[288] Considering the OESC have not yet needed to use the statutory powers under the cyberbullying scheme throughout its years of operation, the question arises whether there is a need for the statutory powers of the OESC under the IBA scheme. However, it is possible that merely having the ability to impose penalties fosters greater compliance. Whether the eSafety Commissioner's statutory power is necessary is discussed in the semi-structured interviews from a stakeholder's perspective so to gain insight into whether the statutory power of the IBSA portal is necessary or excessive. Overall, this 'progressive' and 'collaborative' cyberbullying complaint mechanism has been described as 'effective' and 'important' as it 'reduces strain and pressure on the criminal justice system, and provides timely outcomes for victims'.[289] While the IBA portal has been in operation since 2018 (which is the main focus of this thesis), the success of the cyberbullying complaints scheme can be assessed over a greater period of time and thus provides valuable lessons for those considering the design of a complaints scheme for various forms of harmful online content.

Third described the cyberbullying complaints system as playing a 'critical role', in enhancing Australia's capacity to secure online safety for children and young people, and therefore 'should continue to comprise a key pillar of the Office's work'.[290] However, while the cyberbullying complaints scheme has demonstrated significant merits, a notable limitation of the scheme is its lack of power to formally investigate cyberbullying complaints relating to adults.[291] In 2017-2018, the OESC received requests for assistance from 313 adults who had experienced some form of cyber abuse or cyberbullying.[292] This

[288] Alannah & Madeline Foundation, 'Response to the review into the Enhancing Online Safety Act 2015 and the Online Content Scheme' (August 2018).
[289] Alannah & Madeline Foundation, 'Response to the review into the Enhancing Online Safety Act 2015 and the Online Content Scheme' (August 2018).
[290] Amanda Third, 'Submission to the Review of the Enhancing Online Safety Act 2015 and the Online Content Scheme' (2018).
[291] Women in Media, 'Review of the Enhancing Online Safety Act -Submission' (July 2018) 4.
[292] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2017/18, 124

figure increased by 204 per cent in 2018/2019 to 950 adults.[293] By 2019-2020, the OESC received 1064 requests for assistance from adults experiencing cyber abuse, a further 12 per cent increase from the previous reporting period.[294] In 2020-2021, the OESC received 1599 complaints, a further increase of 52 per cent. In light of these statistics, there is a clear argument in favour of extending the powers of the OESC to complaints of cyberbullying made by adults as well as children. Fortunately, the most recent legislation under the Online Safety Act as explained in section 2.5 established a system for adults to report such issues.[295]

Another limitation of the cyberbullying complaints scheme under the Enhancing Online Safety Act 2015 is that there was uncertainty as to whether certain online service providers that permit the distribution of cyberbullying material were able to be considered as being within the current definition of a social media service in the legislation.[296] With the ever-developing range of technologies and platforms, there was an 'uncertainty as to who and what is in or out of the regulatory regime… making . . . investigation, compliance and enforcement unworkable . . . for the cyberbullying complaints scheme'.[297] In order for this system to be robust, the Online Safety Act 2021 was drafted in a way that was 'technology and platform neutral'.[298] Unlike the cyberbullying complaints scheme in place at the time of the interviews which only applied to content hosted on social media services, the IBSA portal which was implemented subsequent to the cyberbullying complaints scheme applies to intimate images on social media services, designated internet services, hosting services, and internet carriage services.[299] As a result, a broad

[293] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2018/19, 206

[294] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2019/20, 213.

[295] Online Safety Act 2021, Part 7.

[296] Enhancing Online Safety Act 2017, s 4 defines a Social Media Service as follows: (1) For the purposes of this Act, ***social media service*** means: (a) an electronic service that satisfies the following conditions: (i) the sole or primary purpose of the service is to enable online social interaction between 2 or more endusers; (ii) the service allows endusers to link to, or interact with, some or all of the other endusers; (iii) the service allows endusers to post material on the service; (iv) such other conditions (if any) as are set out in the legislative rules; or (b) an electronic service specified in the legislative rules; but does not include an exempt service (as defined by subsection (4) or (5)).

[297] Lynelle Briggs, *Report of the Statutory Review of the Enhancing Online Safety Act 2015 and the Review of Schedules 5 and 7 to the Broadcasting Services Act 1992 (Online Content Scheme)* October 2018, 21.

[298] Lynelle Briggs, *Report of the Statutory Review of the Enhancing Online Safety Act 2015 and the Review of Schedules 5 and 7 to the Broadcasting Services Act 1992 (Online Content Scheme)* October 2018, 21; The Online Safety Act 2021 now applies to a broad range of online services including social media services, relevant electronic services, designated internet services, hosting services and internet service providers. See sections 13, 13(a), 14, 17 & 19.

[299] Enhancing Online Safety Non-consensual sharing of Intimate Images Act 2018

range of services, notably including search engines, fall under the scope of the IBSA portal which came into effect in 2018.

The cyberbullying complaints scheme has been described by members of the industry group, DIGI, as a 'duplication' of existing mechanisms already in place on social media platforms.[300] Members of DIGI assert that the number of reports from the eSafety Commissioner of cyberbullying material hosted on platforms is very low. Members of DIGI claim that the 'very low' number of reports is reflective of the effective nature of the reporting systems they already have in place on their platforms.[301] DIGI have also described the powers granted to the eSafety Commissioner under the cyberbullying complaints as a 'significant deterrent' for social media platforms to take 'independent action'.[302] While such claims must be read in light of the particular interests of the industry group,[303] it remains necessary to establish whether the powers of the eSafety Commissioner have a positive or negative effect on the development of innovative mechanisms for prevention and redress of IBSA. The interviews discussed in Chapter 3 address whether key stakeholders have any criticism of the IBSA civil penalty regime.

2.4.3 Assessing the effectiveness of the eSafety Commissioner's Online Content Scheme – lessons for IBSA

The Online Content Scheme established under schedules 5 and 7 of the Broadcasting Services Act 1992 and administered by the eSafety Commissioner since 2015, regulates offensive and illegal content as described in section 2.3. Before the establishment of the IBSA civil penalty regime under the Enhancing Online Safety Non-Consensual Sharing of Intimate Image Act in August 2018, victims of IBSA could report their intimate images to the 'CyberReport' team of the eSafety Commissioner through the Online Content Scheme. CyberReport investigates reports of harmful online material and acts on material

[300] Digital Industry Group Inc (DIGI), 'DIGI Submission to the review of the Enhancing Online Safety Act 2015' (August 2018) 4.
[301] ibid.
[302] ibid.
[303] ibid.

found to be 'prohibited[304] or potentially prohibited'.[305] Prohibited material categories are defined under the classification guidelines that also apply to offline content such as film. They include child sexual abuse content, content advocating terrorism, instruction, incitement or promotion of crime or violence, and sexually explicit content.[306] Before 2018, victims of IBSA could potentially report their intimate image as being sexually explicit content and therefore prohibited although not all victims of IBSA would fall under this category depending on the content of their intimate image.[307] The removal of an image under this scheme would be entirely unconnected to any harm caused as a result

[304] Broadcasting Services Act 1992, Schedule 7 Part 2 Division 1 Clause 20 defines prohibited material as: (1) For the purposes of this Schedule, content (other than content that consists of an eligible electronic publication) is ***prohibited content*** if: (a) the content has been classified RC or X 18+ by the Classification Board; or (b) both: (i) the content has been classified R 18+ by the Classification Board; and (ii) access to the content is not subject to a restricted access system; or (c) all of the following conditions are satisfied: (i) the content has been classified MA 15+ by the Classification Board; (ii) access to the content is not subject to a restricted access system; (iii) the content does not consist of text and/or one or more still visual images; (iv) access to the content is provided by means of a content service (other than a news service or a current affairs service) that is operated for profit or as part of a profit-making enterprise; (v) the content service is provided on payment of a fee (whether periodical or otherwise); (vi) the content service is not an ancillary subscription television content service; or (d) all of the following conditions are satisfied: (i) the content has been classified MA 15+ by the Classification Board; (ii) access to the content is not subject to a restricted access system; (iii) access to the content is provided by means of a mobile premium service.

[305] Broadcasting Services Act 1992, Schedule 7 Part 2 Division 1 Clause 21 defines potentially prohibited material as: (1) For the purposes of this Schedule, content is ***potential prohibited content*** if: (a) the content has not been classified by the Classification Board; and (b) if the content were to be classified by the Classification Board, there is a substantial likelihood that the content would be prohibited content. (2) However, content is not ***potential prohibited content*** if: (a) the content consists of an eligible electronic publication; and (b) the content has not been classified by the Classification Board; and (c) if the content were to be classified by the Classification Board, there is no substantial likelihood that the content would be classified RC or category 2 restricted. (3) In determining whether particular content is potential prohibited content, it is to be assumed that this Schedule authorised the Classification Board to classify the content.

[306] The National Classification Code defines restricted content as: 1 (a) describe, depict, express or otherwise deal with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that they should not be classified; or (b) describe or depict in a way that is likely to cause offence to a reasonable adult, a person who is, or appears to be, a child under 18 (whether the person is engaged in sexual activity or not); or (c) promote, incite or instruct in matters of crime or violence; The National Classification Code defines category 2 restricted content as: 2 (a) explicitly depict sexual or sexually related activity between consenting adults in a way that is likely to cause offence to a reasonable adult; or (b) depict, describe or express revolting or abhorrent phenomena in a way that is likely to cause offence to a reasonable adult and are unsuitable for a minor to see or read; The National Classification Code defines category 1 restricted content as: 3 (a) explicitly depict nudity, or describe or impliedly depict sexual or sexually related activity between consenting adults, in a way that is likely to cause offence to a reasonable adult; or (b) describe or express in detail violence or sexual activity between consenting adults in a way that is likely to cause offence to a reasonable adult; or (c) are unsuitable for a minor to see or read.

[307] In order for the intimate image to be considered prohibited as per the classification guidelines the image would have to 'depict, express or otherwise deal with matters of sex . . . in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that they should not be classified, explicitly depict sexual or a sexually related activity or explicitly depict nudity'. See Classification (Publications, Films and Computer Games) Act 1995. See also the National Classification Code (May 2005) Intimate images which do not contain nudity or engagement in a sexual activity are excluded such as an image of a person posed in a sexually suggestive position or in underwear or sexually suggestive clothing.

of the image's non-consensual nature. The image would have to depict either sexual intercourse, sexual activities, or nudity, and the non-consensual taking or sharing of the image would be an incidental fact to that assessment. Understanding the effectiveness of the Online Content Scheme in removing harmful online content - most notably sexually explicit content – since 2015 provides insight into the eSafety Commissioner's effect on IBSA prior to the establishment of the IBSA portal.

From the 1st of July 2015 to the 30th of June 2016, the eSafety Commissioner conducted investigations into 11,121 individual items of content.[308] Of the investigations completed, 9,219 items of content were identified as harmful, of which 81% met the definition of child sexual abuse content.[309] However, 1056 items of content were identified as X18+ (explicit sexual content) under the classification scheme and 396 were identified as RC1(a) (refused classification content for a range of matters, including offending against standards of morality and decency and revolting and abhorrent phenomena). Both of these categories may have included cases of IBSA however these specific figures are not published in the eSafety Commissioner's annual reports. Of the 1056 items of X18+ content, eight were hosted within Australia and 1048 hosted outside of Australia. All of the 396 items of RC1(a) content were hosted outside of Australia. While the eSafety Commissioner can request the removal of content hosted overseas, in practice there is little the OESC can do to force the removal of content hosted overseas and as a result in the context of child sexual abuse material the OESC reports these cases to INHOPE.[310] Over 99% of investigations into child sexual abuse material items were completed[311] within two business days.[312] Over 99% of all investigations about prohibited content

[308] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2015/16.

[309] ibid 125.

[310] INHOPE is the global network combatting online Child Sexual Abuse Material (CSAM). The network consists of 50 hotlines in 46 countries that provide the public with a way to anonymously report illegal content online with a focus on CSAM. Reports are reviewed by content analysts who classify the illegality of the material, which is then shared with the national law enforcement agency and a Notice and Takedown order is sent to the relevant hosting provider. See < https://www.inhope.org/EN/the-facts>; INHOPE, Annual Report 2020 < https://inhope.org/media/pages/the-facts/download-our-whitepapers/annual-report/bb4dd3cdc3-1628156678/inhope-annual-report-2020.pdf> accessed 17 January 2022; Office of the eSafety Commissioner, Twenty Years Fighting Child Sexual Abuse; < https://www.esafety.gov.au/newsroom/media-releases/twenty-years-fighting-child-sexual-abuse-online> accessed 17 January 2022.

[311] Completed in this context refers to all child sexual abuse investigations that were finalised (determined to meet the prohibited threshold) and notified to INHOPE or the Australian Federal Police. The meaning of this term was clarified by Natalie Strong, member of the image-based abuse team within the Office of the eSafety Commissioner. See email correspondence with Natalie Strong (Member of the OESC IBS team), on file with author.

[312] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2015/16.

excluding child sexual abuse material were completed within 20 business days.[313] Completed in this context refers the investigations that were finalised (determined to meet the prohibited threshold). During 2015-2016, 12 final take-down notices were issued by the eSafety Commissioner to Australian content hosts. All content that was the subject of a take-down notice was removed by the content host by the end of the next business day as specified under the time frame for removal by the eSafety Commissioner.

During 2016-2017, the eSafety Commissioner conducted investigations into 10,119 individual items of content.[314] Of these investigations, 7,075 items were identified as prohibited or potentially prohibited, of which 72% met the definition of child sexual abuse content.[315] Within the total number of investigations, 1138 items of content were identified as X18+ (explicit sexual content) and 494 were identified as RC1(a) (refused classification content for a range of matters, including offending against standards of morality and decency and revolting and abhorrent phenomena). All of these items were hosted outside of Australia. Over 99% of investigations into child sexual abuse material items were completed within two business days and notified to law enforcement.[316] Similarly to 2015-2016, the completion rate of investigation for all other content including possible IBSA cases was significantly longer - within 20 business days.[317] From 2017-2018, the Office finalised[318] investigations into 13,131 individual items of content.[319] Of these investigations, 10,229 items of prohibited and potentially prohibited content were identified of which 78% met the definition of child sexual abuse content.[320] Unlike previous years, none of these items were found to be hosted in Australia, and so no take-down notices were issued to an Australian content hosts during the reporting period. Within the total number of investigations, 1347 items of content were identified as X18+ (explicit sexual content) and 501 were identified as RC1(a) (refused classification content for a range of matters, including offending against standards of

[313] ibid.
[314] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2016/17, 118.
[315] ibid.
[316] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2016/17, 118.
[317] ibid.
[318] **Finalised:** This refers to all investigations where the content was determined to meet a prohibited classification threshold, i.e. RC1b (CSAM), RC1(a), RC1(c), X18+, R18+. The meaning of this term was clarified by Natalie Strong, member of the image-based abuse team within the Office of the eSafety Commissioner. See email correspondence with Natalie Strong (Member of the OESC IBS team), on file with author.
[319] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2017/18, 127.
[320] ibid.

morality and decency, and revolting and abhorrent phenomena). As per the previous reporting periods, over 99% of investigations into child sexual abuse material were completed within two business days[321] while all other online content complaints were completed within 20 business days.[322]

During 2018-2019, the eSafety Commissioner finalised investigations into 12,126 individual items of content.[323] Of these investigations, 9,242 items were identified as prohibited or potentially prohibited content of which 91 percent met the definition of child sexual abuse material.[324] The 2018/2019 annual report did not include a category for sexually explicit content or refused classification content for a range of matters, including offending against standards of morality and decency and revolting and abhorrent phenomena. The Cyber Report team received no complaints about content from these categories.[325] It is possible that this may be related to the launch of the IBSA reporting mechanism. No take-down notices were issued to Australian content hosts during this period as none of the content was hosted in Australia. Over 99 per cent of investigations into child sexual abuse content items were completed within two business days.[326] Over 99 per cent of all investigations about online content except for child sexual abuse content were completed within 20 business days.[327] These figures are the same as the previous period.

There were 13,484 items which met the threshold of prohibited or potentially prohibited content in the reporting period of 2019-2020. Of these items, 99 percent met the definition of child sexual abuse material. Similar to 2018-2019, none of the material was hosted in Australia therefore no takedown notices were issued. The time frames for completed investigations were the same as the previous reporting period. Once again, the 2019-2020 and 2020-2021 reporting period did not include a category for sexual or sexually explicit content or refused classification content for a range of matters, including offending against standards of morality and decency, and revolting and abhorrent phenomena.

While the above data from the eSafety Commissioner's annual reports provides insight into the time frames for the conducting of investigations into harmful online content it

[321] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2017/18.
[322] ibid.
[323] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2018/19.
[324] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2018/19.
[325] ibid.
[326] ibid.
[327] ibid.

does not release the time frame from when a report is made and to when the harmful material is removed. This specific time frame is important as the timely removal of the harmful content reduces the potential of revictimization, and the possibility of the material being distributed further. Interviews discussed in Chapter 3 assess whether the OESC is perceived to be acting in a timely manner.

A question must also be posed as to whether 20 days – in the case of all material prohibited under the classification code excluding child sexual abuse material – is too long to complete an investigation considering investigations into child sexual abuse material specifically can be conducted within two days. While it seems appropriate to prioritise investigations into child sexual abuse material due to the immense harm associated, the difference in timelines may highlight a need for greater resources to conduct investigations which are not related to child sexual abuse in a fast and effective manner. This point was highlighted by Third who stated 'resources are tight and sometimes hinder the capacity of the office to respond to the breadth of issues within their mandate'.[328] The legislation governing the Online Content Scheme (schedules 5 and 6 of the Broadcasting Services and Act and the Enhancing Online Safety Act 2015) have been described as 'piecemeal'[329] and lacking in 'coherence and consistency'.[330] As a result, the online content scheme was deemed 'not fit for purpose'.[331] This argument was previously made in 2012 by the Australian Law Reform Commission stating that the Broadcasting Services Act provisions regulating online content were 'highly complex', 'confusing' and 'legally uncertain'.[332] Considering the complex nature of the legislation upon which the eSafety Commissioner must abide by, this may hinder their ability to be fully effective.

The Online Content Scheme proves effective when removal notices are issued for content hosted within Australia as all removal requests are implemented. However, considering the majority of the content is hosted outside of Australia where a removal notice lacks force, the question arises as to the outcome of these reported complaints. As the annual reports do not address this issue, Chapter 3 discusses how the eSafety Commissioner response attempts to remove or reduce the visibility of harmful content including intimate images hosted outside of Australia.[333]

---

[328] Amanda Third, 'Submission to the Review of the Enhancing Online Safety Act 2015 and the Online Content Scheme' (2018).

[329] Lynelle Briggs, *Report of the Statutory Review of the Enhancing Online Safety Act 2015 and the Review of Schedules 5 and 7 to the Broadcasting Services Act 1992 (Online Content Scheme)* October 2018, 10.

[330] ibid.

[331] ibid.

[332] Australian Law Reform Commission, *Classification — Content Regulation and Convergent Media* (Report 118 — 2012) 58.

[333] See Chapter 3, section 3.6.2.

2.4.4 Assessing the effectiveness of the eSafety Commissioner's Image Based Abuse Portal

In October 2017, the OESC launched the IBA Portal providing reporting options, support and educative resources to Australians who have experienced IBSA. This function was expanded in September 2018, empowering the eSafety Commissioner with statutory power to enforce the removal of intimate images as explained in section 2.3.8.2. Although the IBA Portal is relatively new, it has received widespread support, international acclaim, and domestic recognition as the 'key point of referral for support services' in addition to it providing the entry point to the administrative complaints scheme.[334] Franks described the portal as 'the most comprehensive resource on this issue'[335] and the Department of Home Affairs described the expanded powers as a 'valuable tool'.[336]

Between the 17th of October 2017 and the 30th of June 2018, the eSafety Commissioner received 259 reports of IBSA through its IBA Portal.[337] These reports related to 401 separate URLs where the IBSA material was available across 130 different platforms.[338] The eSafety Commissioner was successful in having IBSA material voluntarily removed in 80% of cases where removal was requested (but where no formal removal noticed was issued), despite the material being hosted overseas and the lack of statutory power to enforce any non-compliance notices.[339]

During the reporting period of 2018/2019,[340] the eSafety Commissioner received 950 reports of IBSA representing a substantial increase of 691 reports compared to the previous reporting period.[341] Of the 950 received, 849 reports of IBSA were received between the 1 September 2018 and 30 June 2019. The civil penalty regime was introduced on the 1st of September 2018. The eSafety Commissioner also received 241 enquiries

[334] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2017/18.
[335] Sarah Ashley O'Brien, 'Australia takes on revenge porn', *CNN* (New York, 16 October 2017).
[336] Department of Home Affairs, 'Review of the Enhancing Online Safety Act 2015 and the Online Content Scheme' (August 2018).
[337] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2017/18.
[338] ibid.
[339] ibid.
[340] Same as the Australian Financial year – 1st July 2018 to 30th June 2019. Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2018/19, 203.
[341] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2018/19, 207.

about IBSA and over 136,450 visits to its image-based abuse portal.[342] The significant increase in reports to the IBA portal would suggest an increase in awareness about the portal. During the 2018/2019 reporting period, the eSafety Commissioner requested removal of IBSA material from over 1,700 locations where the material was available across 130 different platforms.[343] The eSafety Commissioner's success rate increased from the previous reporting period and was successful in having IBSA material removed in 90 per cent of cases where removal was requested and no formal removal notice was issued, despite the majority of material being hosted overseas. The majority of the material was posted on pornography sites. Only a small portion of reports concerned material posted on social media sites.[344]

As regards actions taken against persons responsible for IBSA, the eSafety Commissioner issued one formal removal notice (which was complied with), three formal warnings, and eight informal warnings.[345] The eSafety Commissioner stated that it was 'adopting an educative approach to enforcement in appropriate cases given the newness of the civil penalties scheme'.[346]

During the reporting period of 2019-2020 there was a 184 per cent increase in the number of reports received through the IBSA portal, amounting to 2702 reports.[347] Between March and May 2020, following the introduction of the first Covid-19 restrictions, there was a particular spike in IBSA reporting with this period accounting for 1000 reports of the 2702 total reports received.[348] Nearly 60 percent of these reports related to a sextortion email scam whereby victims were threatened with the release of compromising footage unless an amount was paid in Bitcoin. In response to reports received in 2019-2020, the OESC issued seven removal notices to websites and hosting providers, all based outside of Australia.[349] Five out of the seven removal notices were complied with.[350] In the two cases where the notice was not complied with, as the OESC does not have extraterritorial powers the OESC took steps to 'limit the discoverability of the content, typically by removing the content from search engine results',[351] this was done by requesting search

[342] ibid.
[343] ibid 209.
[344] ibid 209.
[345] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2018/19, 208.
[346] ibid.
[347] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2019/2020, 214.
[348] ibid.
[349] ibid.
[350] ibid.
[351] ibid.

engines to voluntarily de-index the content from their server. The OESC also issued four formal warnings to persons responsible for IBSA and one informal warning to a person where the OESC felt that 'an educative approach to enforcement' was more appropriate.[352] During the 2019-2020 reporting period, the eSafety Commissioner requested removal of IBSA material from over 4000 locations, mainly URLs (an increase of 3300 locations from the previous reporting period) where the material was available across 248 different platforms (compared to 130 platforms in the previous reporting period). [353] The eSafety Commissioner was successful in having IBSA material removed in 82 per cent of cases where removal was requested. This is an 8 per cent decrease from the previous reporting period.

During the reporting period of 2020-2021, the OESC received 2687 reports of IBSA, a slight decrease from the previous reporting period.[354] The most common behaviour reported was 'sextortion' which amounted to 57 per cent of reports received.[355] In response to reports received, the eSafety Commissioner issued one formal removal notice which was to a website hosted overseas, two remedial directions, and two warnings.[356] During the 2020-2021 reporting period, the eSafety Commissioner requested removal of IBSA material from over 2500 locations, mainly URLs (a decrease of 1500 locations from the previous reporting period) where the material was available across 141 different platforms.[357] The eSafety Commissioner was successful in having IBSA material removed in 90 per cent of cases through informal action. This is an 8 per cent increase from the previous reporting period.[358]

Although no civil penalties have been imposed thus far, the statutory powers afforded to the eSafety Commissioner under the Enhancing Online Safety Non-consensual Sharing of Intimate Images Act 2018[359] are envisaged to 'reduce strain and pressure on the criminal justice system'[360] by providing 'further enforcement options'.[361] The industry

[352] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2019/20, 214.
[353] ibid 216.
[354] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2020/21, 212.
[355] ibid 213.
[356] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2020/21, 215.
[357] ibid.
[358] ibid.
[359] As outlined in section 4.3.8.2.
[360] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2017/18.
[361] ibid.

group DIGI argues that aspects of the expanded powers should be left to law enforcement agencies that are experienced in the legal process involved in determining guilt and intent.[362] While it is not unexpected that an industry group is opposed to increased regulation, a need remains to understand how the eSafety Commissioner determines what reported cases should be notified to police authorities. These issues are considered during the interviews as discussed in Chapter 3. It is also unsurprising that members of DIGI strongly advocated for a 'carve-out' to insulate providers from intermediary liability where they provide 'prompt and effective' removal processes for intimate images.[363] As this liability safe harbour was not adopted, DIGI members argue there is a 'discouragement for digital platforms and service providers to continue to invest in such solutions'[364] such as removal processes and technological solutions. While DIGI did not provide any evidence for this contention, industry groups are of course generally in favour of self-regulation.[365] This position was considered in the interviews discussed in Chapter 3. A key theme of the interviews was whether existing social media policies are effective in practice and what is the additional value of the eSafety Commissioner's statutory powers.

There is a lack of information published about the success of the eSafety Commissioner in assisting in the removal of intimate images permanently – or for an extended period – and it does not appear that the eSafety Commissioner has a system for recording and reporting reoccurring abuse. One question explored in the interviews (discussed in Chapter 3) was whether the IBSA material reported to the eSafety Commissioner tends to remain offline or resurfaces in a short time period. Furthermore, the interview questions sought additional detail regarding the average time between the eSafety Commissioner receiving a report of IBSA to when the IBSA material is removed.

2.4.5 Overall Assessment of the eSafety Commissioner Based on Available Evidence: Lessons and Issues to Explore in Interviews

The discussion above highlights some of the merits and limitations of the eSafety Commissioner's role in the combating of IBSA and other forms of online harm. The eSafety Commissioner's annual reports and the Briggs report – and related submissions

[362] Digital Industry Group Inc (DIGI), 'DIGI Submission to the review of the Enhancing Online Safety Act 2015' (August 2018) 3.
[363] ibid.
[364] ibid.
[365] See discussion in Chapter 1 section 1.6.

– provide invaluable information and insight into the operation of the eSafety Commissioner. Despite this, additional exploration is required in order to assess the effectiveness of the eSafety Commissioner in practice and from different perspectives. Below is an overview of the key findings and lessons learned from the desk-based assessment of the eSafety Commissioner.

The educative and awareness-raising functions of the eSafety Commissioner – including the educational functions of the website, virtual classrooms, outreach programmes, eSafetyWomen and collaborative relationships – have all recorded an increase in the number of people viewing, using, or participating with these resources since 2015 to 2020. However, there is no information indicating who is engaging with these resources or how they are using them. Accordingly, the interviews explore whether IBSA victims and associated stakeholders are aware of the resources, programmes, and reporting mechanisms available. The aim is to establish whether the high levels of engagement reported in the annual reports are reflective of the experiences of the interviewed stakeholders. The interviews also aim to ascertain the public visibility of the OESC and general awareness of its functions. Furthermore, while the eSafety Commissioner engages in collaborative relationships, notably through the Trusted eSafety Providers scheme, there is no information provided as to the number of referrals made by the eSafety Commissioner to the Trusted eSafety Providers nor the level of collaboration that exists. An aim of the interviews discussed in Chapter 3 was to gain some insight into this issue through discussion with the Alannah and Madeline Foundation, a registered Trusted eSafety Provider. Due to the number of website visitors, social media followers, and newsletter subscribers, there seems to be strong general awareness of the eSafety Commissioner. However, it is unknown whether these and other awareness raising actions such as media campaigns are reaching victims of IBSA. Knowing whether victims and stakeholders are aware of the OESC and its powers and processes will assist the assessment of the effectiveness of the OESC educative role. Therefore, the interviews aim to establish whether stakeholders and victims of IBSA are aware of the OESC and its functions including its educative and awareness raising roles and reporting mechanisms.

The Cyberbullying Complaints Scheme was the first reporting mechanism examined in order to help assess the eSafety Commissioner's effectiveness in bringing about the removal of harmful online content. This reporting mechanism was analysed as it has been in place for longer than the IBSA reporting mechanism and therefore has more data points. Overall, evidence provided in the annual reports demonstrates a trend of increasing numbers of reported cases of cyberbullying material and reducing time periods

for removal. Notwithstanding this, additional information on whether the removed material during these reporting periods remained offline or whether there were cases of revictimization by the material resurfacing or whether the OESC seeks to keep track or maintains records of such activity would be beneficial. As a result, Chapter 3 explores whether the interviewed stakeholders had insight into this or any thoughts as to how this informational gap could be addressed.

Lessons learned from examining the processes and outcomes applicable in the cyberbullying and other harmful material contexts helps inform assessment of the IBSA regime. Adopting a collaborative approach, the eSafety Commissioner has developed relationships with social media platforms which has facilitated the timely removal of cyberbullying material. The cooperative relationships built with intermediaries have also reduced the need to take statutory action under the cyberbullying complaints scheme. A question asked in the interviews is whether there is a need for the IBSA portal to have statutory power considering the cyberbullying complaints scheme has not needed to utilise its statutory powers. The industry group, DIGI, have argued in their submission to the review of the Enhancing Online Safety Act 2015 that the scheme may be a deterrent to independent actions such as social media policies and technology-based solutions. [366] Bearing this contention in mind, the interviews provided an opportunity to explore the significance and purpose of the statutory powers with experts – including with some with a more critical perspective of the industry position.

The second reporting mechanism assessed was the Online Content Scheme. Before the establishment of the IBA portal, victims of IBSA could have, in certain limited circumstances, reported their intimate image to the eSafety Commissioner through the Online Content Scheme. The annual reports of the eSafety Commissioner contain some information breaking down the reported material into categories – for example child sexual abuse material – but no specific figures were reported for IBSA cases under this scheme. This is not surprising as IBSA is not a category of relevance to the Online Content Scheme. Of the indecent sexual material reported (which could have included cases of IBSA) it took the eSafety Commissioner up to 20 days to complete an investigation. However, there is no data published on the time frame from when the material is reported to when the material is removed. Through conducting the interviews

[366] Digital Industry Group Inc (DIGI), 'DIGI Submission to the review of the Enhancing Online Safety Act 2015' (August 2018).

discussed in Chapter 3, the author sought insight from participants as to whether in their experience, material was removed in a timely manner following eSafety Commissioner action. Of the cases reported under the Online Content scheme, most of the content was hosted outside of Australia. While content hosted within Australia was removed in the majority of cases, the removal of content hosted outside of Australia was less successful due to challenges in imposing an enforcement action. However, in these situations the OESC reported the material to INHOPE in the context of CSAM or the Federal Police. Due to the challenges with seeking the removal of content hosted overseas, questions asked in the interviews sought to establish whether the OESC had an alternative response where jurisdictional challenges arose such as reducing the visibility of the content within Australia. The final reporting mechanism assessed was the IBA portal. As this reporting mechanism is the newest addition, there was less data available to conduct an in-depth desk-based assessment. However, the IBSA portal is of most relevance to this thesis and warranted intense examination of the available data. Furthermore, as the IBA scheme is a relatively new system, there is a limited amount of data available to access its performance, as a result there is a great need for interviews to supplement gaps in the available evidence.

While the annual reports show that the majority of intimate images reported to the eSafety Commissioner are removed from the internet, it is unknown whether the reported material remains offline permanently or for an extended period of time or if the eSafety Commissioner seeks to keep track of such information. One question explored in the interviews was whether the eSafety Commissioner has a system to identify reoccurring abuse. The speedy removal of intimate images is vital to avoid the consequences of rapid sharing common on the 'viral' internet. As the annual reports did not disclose the average time between the eSafety Commissioner receiving a report of IBSA to when the intimate image was removed, the interview questions sought additional detail to address this gap. As the eSafety Commissioner is unsuccessful in assisting in the removal of reported IBSA content in some cases, the interview questions sought to understand whether the eSafety Commissioner takes any alternative measures to reduce the harm and provide alternative support to victims.

As outlined above, the expanded statutory powers of the OESC to issue removal notices has been regarded as a valuable tool to reduce the strain on the justice system. However, a report from the Digital Industry Group Inc questioned whether the eSafety Commissioner is equipped to make decisions on what content should warrant a removal notice. Questions in the interviews aimed to address how the eSafety Commissioner

determines what images should be removed and what images should be reported to police authorities. The industry group also advocated for a 'carve out' for intermediaries who already had policies for the removal of IBSA material. Questions in the interviews prompted discussion on whether existing social media policies are sufficient and what is the additional value of the eSafety Commissioner's statutory powers.

2.5 The current governing legislation – Online Safety Act 2021

2.5.1 Introduction

In June 2018, the then Minister for Communications in Australia (Senator Mitch Fifield) announced an independent review of Australia's online safety legislation. This review examined the Enhancing Online Safety Act 2015 and Schedules 5 and 7 of the Broadcasting Services Act 1992.[367] As mentioned previously in this chapter, Briggs conducted the review and reported that although current regulatory arrangements for online safety had been effective, major reform was needed to strengthen the regulatory regime and align it with community expectations, including replacing the existing framework (as outlined in this chapter and discussed in the interviews in Chapter 3) with a single Online Safety Act.[368] Following substantial public and stakeholder consultation,[369] the Online Safety Act was passed in June 2021 and came into force on the 23rd of January 2022.

2.5.2 Overview of the Online Safety Act

The Australian government enacted the Online Safety Act 2021 to better equip the OESC to prevent and address current and future online harms in a rapidly changing environment.[370] The Act enhances the OESC regulatory mechanisms already established under the Enhancing Online Safety Act 2015 for dealing with IBSA,[371] the cyberbullying

[367] Senator the Hon Mitch Fifield, Minister for Communications, 'New reviews of online safety for Australians', (Media Release, 26 June 2018).
[368] Lynelle Briggs, *Report of the Statutory Review of the Enhancing Online Safety Act 2015 and the Review of Schedules 5 and 7 to the Broadcasting Services Act 1992 (Online Content Scheme)* October 2018.
[369] Department of Infrastructure, Transport, Regional Development and Communications, 'Consultation on Online Safety Reforms', < www.communications.gov.au/have-yoursay/consultation-online-safety-reforms > accessed 26 February 2021; Online Safety Bill 2021, Explanatory Memorandum; Department of Infrastructure, Transport, Regional Development and Communications, 'Consultation on a Bill for a new Online Safety Act' < www.communications.gov.au/have-yoursay/consultation-bill-new-online-safety-act > accessed 26 February 2021.
[370] Office of the eSafety Commissioner, *eSafety Regulatory Posture and Regulatory Priorities 2021-22* (November 2021).
[371] Online Safety Act 2021, Part 6.

of children,[372] and illegal or restricted online content,[373] while also introducing a new scheme for dealing with adult cyber abuse.[374] In particular the Act strengthens these schemes and brings them into greater alignment with each other. For example, under the Act, each scheme now applies to a broad range of online services including social media services,[375] relevant electronic services,[376] designated internet services,[377] hosting services,[378] and internet service providers.[379] Also, the services have a standard 24-hour time period to comply with removal notices. The Online Safety Act also allows for the development of 'Basic Online Safety Expectations' for a broad range of online services, outlining the fundamental safety practices expected of service providers.[380] By empowering the OESC to request or require information about how services are protecting the online safety of their users, it is envisaged the expectations will 'drive greater transparency and accountability'.[381]

Section 27 of the Act sets out the functions of the OESC. These functions remain the same as Section 15 of the Enhancing Online Safety Act 2015. However, the powers of the OESC have expanded and the regulatory schemes of the OESC are set out under Section 29 of the Act which provides a simplified outline of Part 3 of the Act as follows:

> • There is a complaints system for cyber-bullying material targeted at an Australian child.
>
> • There is a complaints and objections system for non-consensual sharing of intimate images.
>
> • There is a complaints system for cyber-abuse material targeted at an Australian adult.
>
> • There is a complaints system relating to the online content scheme.[382]

[372] ibid Part 5.
[373] ibid Part 9.
[374] ibid Part 7.
[375] ibid s13.
[376] ibid s 13(a).
[377] ibid s 14.
[378] ibid s17.
[379] ibid s 19.
[380] ibid Part 4.
[381] Office of the eSafety Commissioner, *eSafety Regulatory Posture and Regulatory Priorities 2021-22* (November 2021).
[382] Online Safety Act 2021, s 29.

2.5.3 The Online Safety Act in the context of image-based sexual abuse

The Online Safety Act enhances the image-based abuse scheme already established under the Enhancing Online Safety Act 2015. The Online Safety Act was described in the explanatory memorandum as making 'modest reforms to the already successful image-based abuse scheme' so to 'further mitigate this harm' for all Australians.[383] In particular these reforms include a reduced timeframe from 48 hours to 24 hours upon which an intimate image must be removed upon the receival of a removal notice. Furthermore, the Act provides enhanced protection for cases of sextortion and images of victims without religious or cultural attire and also considers new types of technologies used against victims such as deepfakes or intimate images that purport to be of a person.

The enhanced image-based abuse scheme can be described as having key 'regulatory features'.[384] The Act provides for the general prohibition of IBSA. It provides a system under which a person may make a complaint for breaches of the general prohibition. It provides a system under which a person may object to an intimate image remaining online even if the person depicted originally consented to the intimate image being shared. It provides the OESC with investigative and information gathering powers. Finally, it also affords the OESC powers to issue removal notices, remedial directions, and enforcement actions. These features will be explained in greater detail in the following sections so to provide a comprehensive overview on how the Online Safety Act 2021 protects against IBSA while also clearly identifying how the protection for IBSA has evolved.

2.5.3.1 The general prohibition of image-based sexual abuse

Section 15 of the Online Safety Act sets out the definition of an intimate image. Unlike the Enhancing Online Safety Act 2015, this definition is divided into three categories including images depicting private parts, private activities, and people without religious attire. Section 15 states:

> (1) This section sets out the circumstances in which material is an intimate image of a person for the purposes of this Act.
> *Depiction of private parts*
> (2) Material is an intimate image of a person if:
> (a) the material consists of a still visual image or moving visual images; and
> (b) the material depicts, or appears to depict:

[383] Online Safety Bill 2021, Explanatory Memorandum.
[384] Office of the eSafety Commissioner, *eSafety Regulatory Posture and Regulatory Priorities 2021-22* (November 2021).

(i) the person's genital area or anal area (whether bare or covered by underwear); or

(ii) if the person is a female person or a transgender or intersex person—either or both of the person's breasts; in circumstances in which an ordinary reasonable person would reasonably expect to be afforded privacy.

Depiction of private activity

(3) Material is an intimate image of a person if:

(a) the material consists of a still visual image or moving visual images; and

(b) the material depicts, or appears to depict, the person:

(i) in a state of undress; or

(ii) using the toilet; or

(iii) showering; or

(iv) having a bath; or

(v) engaged in a sexual act of a kind not ordinarily done in public; or

(vi) engaged in any other like activity;

in circumstances in which an ordinary reasonable person would reasonably expect to be afforded privacy.

Depiction of person without attire of religious or cultural significance

(4) Material is an intimate image of a person if:

(a) the material consists of a still visual image or moving visual images; and

(b) because of the person's religious or cultural background, the person consistently wears particular attire of religious or cultural significance whenever the person is in public; and

(c) the material depicts, or appears to depict, the person:

(i) without that attire; and

(ii) in circumstances in which an ordinary reasonable person would reasonably expect to be afforded privacy.[385]

Furthermore, unlike the Enhancing Online Safety Act, the new legislation provides stronger protection for images whereby the person is not necessarily in the image but is depicted in the image. Also, the new legislation provides clear guidance that images which have been altered such as deepfakes also fall within the scope of the definition of an intimate image. Section 15 parts 5 and 6 states:

Interpretative provisions

(5) For the purposes of this section, it is immaterial whether material has been altered.

(6) For the purposes of this section, if material depicts, or appears to depict, a part of the body of a person, the material is taken to depict the person, or to appear to depict the person, as the case requires.[386]

[385] Online Safety Act 2021, s 15.

[386] ibid.

The general prohibition of image-based abuse is the same as that in the Enhancing Online Safety Act 2015 however it is more inclusive due to the wider definition of an intimate image. Section 75 allows the OESC to take action against a person (end-user) who shares or threatens to share an intimate image without the consent of the person shown.[387] It is a civil penalty provision which is punishable by up to 500 penalty units.[388] Section 75 states:

> Posting an intimate image
> (1) A person (the first person) who is an end-user of:
> (a) a social media service; or
> (b) a relevant electronic service; or
> (c) a designated internet service; must not post, or make a threat to post, an intimate image of another person (the second person) on the service if:
> (d) the first person is ordinarily resident in Australia; or
> (e) the second person is ordinarily resident in Australia.
> Civil penalty: 500 penalty units[389]

2.5.3.2 Making a complaint to the OESC

Similar to the Enhancing Online Safety Act 2015, Section 32 of the Online Safety Act allows a person who is depicted in an intimate image or an authorised person to report a contravention of the general prohibition of IBSA as set out under Section 75. In other words, a person can make a complaint to the OESC through the IBA portal if another person has posted or threatened to post an intimate image of them. A person making a complaint does not need to have reported the image to the online service provider where it appeared before making a complaint to the OESC.[390] Also, a person can still make a complaint even if they cannot identify the person who shared the intimate image.[391] Once a complaint is received, the OESC is empowered to conduct an investigation and consider compliance and enforcement actions which will be outlined in section 2.5.3.6 and 2.5.3.7.

2.5.3.3 Making an objection to the OESC

[387] ibid s 75(1).
[388] The monetary value of 1 penalty unit is still $222 (until 30 June 2023) for individuals. In addition, the maximum penalty ordered against a corporation (which can include online service providers) can be 5 times more than the maximum penalty ordered against an individual.
[389] Online Safety Act 2021, s 75(1).
[390] Office of the eSafety Commissioner, *eSafety Regulatory Posture and Regulatory Priorities 2021-22* (November 2021).
[391] Online Safety Act 2021, s 32(2).

While a victim of IBSA may want to report a case of IBSA so to ensure the removal of the image by the end user or prevention of the posting of the image by the end user in the first place, a victim may also want to ensure their image is not being hosted on a platform. Furthermore, a person may at one stage have consented to the posting of an intimate image of them but later would like to retract that consent. They would not be able to make a complaint under Section 32 as the poster of the image did not contravene Section 75 (as the image was posted with consent). Instead, the person can make an objection notice to the OESC objecting to the provision of their intimate image on a particular platform(s). An objection notice may be made by the person depicted in the image or an authorised person. Section 33 states:

> (1) If a person (the depicted person) has reason to believe that:
> (a) an intimate image of the depicted person is, or has been, provided on:
> (i) a social media service; or
> (ii) a relevant electronic service; or
> (iii) a designated internet service; and
> (b) the provision of the intimate image on the service is not an exempt provision of the intimate image; and
> (c) any of the following conditions is satisfied:
> (i) the depicted person is ordinarily resident in Australia;
> (ii) if the intimate image was posted on the service by an end-user of the service—the end-user is ordinarily resident in Australia;
> (iii) the intimate image is hosted in Australia by a hosting service;
> the depicted person may give the Commissioner a notice (an objection notice) objecting to the provision of the intimate image on the service.[392]

Upon receiving an objection notice, the OESC may conduct an investigation and consider whether to issue a removal notice to the relevant service(s) which will be explained in section 2.5.3.6.2.

2.5.3.4 Investigations by the OESC

Section 34(1) grants the OESC the power to investigate complaints and objection notices in relation to IBSA. The OESC investigative powers are set out in Part 14 of the Act. These powers include the ability to compel a person to answer questions and/or produce documents or other information as requested by the OESC.[393] Furthermore, the OESC has additional information-gathering powers as set out under Part 13 of the Act. Section 194 allows the OESC to obtain end-user identity and contact information from a social media service, relevant electronic service or designated internet service, if the OESC has

[392] ibid s 33.
[393] ibid s 197 to s 205.

reason to believe that the information is, or the contact details are, relevant to the operation of an investigation.[394] Failure to comply with such a request would result in a civil penalty of 100 penalty units.[395]

2.5.3.5 Approaches to compliance and enforcement

Similar to the Enhancing Online Safety Act 2015, the Online Safety Act provides the OESC with a range of formal compliance and enforcement options in response to IBSA. The OESC may also consider making informal requests as well. The formal compliance responses available to the OESC include service provider notifications (can be issued to a provider of a social media service, relevant electronic service or designated internet service), removal notices (can be issued to a provider of a social media service, relevant electronic service or designated internet service and an end user), and remedial directions (can be issued to an end user). The enforcement options available to the OESC for failure to comply with any of the above notices or directions include the issuing a formal warning, the accepting of an enforceable undertaking, the seeking of a court injunction, the issuing of an infringement notice or the seeking of a civil penalty order. The various compliance notices and enforcement actions are explained below.

2.5.3.6 Compliance notices

2.5.3.6.1 Service provider notifications

Section 85 of the Act allows the OESC to issue a service provider notification to the provider of a social media service, relevant electronic service or designated internet service. A service provider notification informs the online service provider that the OESC is aware that it is hosting an intimate image and that the OESC has received a complaint or objection about the intimate image.[396] A service provider notification can be issued in two circumstances. The first circumstance includes a written notice from the OESC to the service provider making the provider aware of the intimate image on its service therefore notifying the provider that it is 'on notice'.[397] The OESC would expect that the notice would prompt the service provider to remove the material in a fast manner. The OESC describes this as a 'a less formal approach' compared to a removal notice which is

[394] ibid s 194.
[395] ibid s 195.
[396] ibid s 85.
[397] ibid s 85(1).

envisaged to result in faster content removal.[398] This type of service provider notification can only be issued with the consent of the person making the complaint or the objection notice.[399] It does not give rise to enforcement options if the online service provider does nothing in response to the notice. [400] Section 85(2) provides for the second circumstance in which the OESC can issue a service provider notification under the image-based abuse scheme. Under Section 85(2), the OESC may provide a statement to an online service provider where an intimate image of a person is, or was, available on the service on two or more occasions over the past 12 months.[401] Furthermore, in order to issue this statement, the material must also have breached the service's own terms of use.[402] The OESC may also publish this statement on its website.[403] The purpose of publishing this statement is to 'name and shame' services that are not doing enough to combat IBSA.[404]

2.5.3.6.2 Removal notices

Section 77 allows the OESC to issue a removal notice which is a written notice requiring the recipient to take all reasonable steps to remove an intimate image from a service within 24 hours or a longer timeframe specified by eSafety.[405] This is a reduced time frame compared to the 48 hours under the Enhancing Online Safety Act. A removal notice may be issued if an intimate image is posted on a service providers platform and contravenes the general prohibition under Section 75 or was the subject of a complaint or objection notice.[406] A removal notice may be issued to an end user[407] and/or the provider of a social media service, relevant electronic service, designated internet service.[408] Failure to comply with a removal notice will result in a civil penalty of 500 units.[409] The failure also enables the OESC to take a range of enforcement actions as outlined below in section 2.5.3.7.

---

[398] Office of the eSafety Commissioner, *eSafety Regulatory Posture and Regulatory Priorities 2021-22* (November 2021).
[399] Online Safety Act 2021, s 85(1).
[400]Office of the eSafety Commissioner, *eSafety Regulatory Posture and Regulatory Priorities 2021-22* (November 2021).
[401] Online Safety Act 2021, s 85(2).
[402] ibid s 85(2)(b).
[403] ibid s 85(2)(f).
[404] Office of the eSafety Commissioner, *eSafety Regulatory Posture and Regulatory Priorities 2021-22* (November 2021).
[405] ibid s 77.
[406] ibid s 77.
[407] ibid s 78.
[408] ibid s 79.
[409] ibid s 80.

2.5.3.6.3 Remedial directions

Section 83 of the Online Safety Act allows the OESC to issue a written direction to an end user requiring that person to take specified action directed towards ensuring that the person does not contravene Section 75 in the future.[410] A remedial direction is suitable where a removal notice is insufficient to address the risk of future abuse. For example, if a person has threatened to post an intimate image, the OESC may direct the person not to do so and to delete the image from their device.[411] Failure to comply with a remedial direction may result in a civil penalty of up to 500 penalty units.[412] The failure also enables the OESC to take a range of enforcement actions as outlined below in section 2.5.3.7.

2.5.3.7 Enforcement actions

The OESC may take an enforcement action against an end-user who has failed to comply with the general prohibition under Section 75, a removal notice under Section 77, or a remedial direction under Section 83. The OESC may take an enforcement action against an online service provider who has failed to comply with a removal notice under Section 78. The enforcement actions available to the OESC remain the same as those available under the Enhancing Online Safety Act 2015 and include enforceable undertakings[413], injunctions[414], infringement notices[415] and civil penalty orders[416].

2.5.3.8 Review rights

Section 220 and 220(a) allows a decision of the OESC to issue a removal notice against a service provider or end user or a remedial direction against an end user to be subject to an internal review by the OESC and an external review by the Administrative Appeal Tribunal. Furthermore, if the OESC refuses to issue a removal notice following a valid complaint, the person who made the complaint can request a review of this decision.[417]

---

[410] ibid s 83.
[411] Office of the eSafety Commissioner, *eSafety Regulatory Posture and Regulatory Priorities 2021-22* (November 2021).
[412] Online Safety Act 2021, s 83(3).
[413] ibid s 164.
[414] ibid s 165.
[415] ibid s 163.
[416] ibid s 162.
[417] ibid s 220.

2.5.3.9 Annual reports

Section 183(1) of the Act requires the OESC to release an annual report. This was also required by the previous legislation however Section 183(2) of the new Act specifies certain data to be included in the annual report. In the context of IBSA, such data includes: the number of objection notices made, the number of complaints received, the number of removal notices, remedial directions, link deletion notices, and app removal notices issues, and the number of decisions reviewed, and applications received for internal review. The following parts of Section 183(2) have direct relevance to IBSA:

> (2) A report under subsection (1) relating to a financial year must set out the following:
> (aa) the number of objection notices given to the Commissioner under section 33 during that year;
> (f) the number of notices given by the Commissioner under section 77 during that year;
> (g) the number of notices given by the Commissioner under section 78 during that year;
> (i) the number of directions given by the Commissioner under section 83 during that year;
> (t) the number of notices given by the Commissioner under section 124 during that year;
> (u) the number of notices given by the Commissioner under section 128 during that year;
> (ze) the number of decisions that were reviewed by the Commissioner under the internal review scheme (see section 220A) during that year;
> (zf) the number of applications that were received by the Commissioner under the internal review scheme (see section 220A) during that year;
> (zh) the number of informal notices given, and informal requests made, by the Commissioner to a person in relation to non-consensual sharing of intimate images during that year;
> (zn) the number and percentage of complaints made to the Commissioner during that year for non-consensual sharing of intimate images by ground or category of harm, with such grounds or categories of harm to be determined by the Commissioner;[418]

2.5.3.10 Changes to the Online Content Scheme that effect IBSA

The Online Content Scheme which was previously provided for under Schedules 5 and 7 of the Broadcasting Services Act is now included in the Online Safety Act. The Online Content Scheme provides a system whereby a complaint can be made about online material that a person believes to be illegal or should be restricted. The OESC uses the term 'illegal and restricted online content' to refer to online content that can either be

[418] ibid s 183(2).

defined as ‘class 1 material’ or ‘class 2 material’ which are defined by reference to Australia’s National Classification Scheme. Some cases of IBSA (particularly in the context of sexual activity) may fall under either of these categories as previously described in section 2.4.3. In the context of IBSA, there are two particular powers under the Online Content Scheme afforded to the OESC under the new legislation which may impact the regulation of IBSA. The Online Safety Act allows the OESC to request the removal of access to class 1 material. They may impact on content hosted overseas. Section 124 of the Online Safety Act allows the OESC to issue a link deletion notice which is a written notice requiring the provider of an internet search engine service to stop providing a link that gives Australian users access to class 1 material within 24 hours or a longer time frame specified by the OESC.[419] In order to issue a link notice the provider of the search engine service must have allowed access to the link to the class 1 material on two or more occasions in the past 12 months and received one or more removal notices in relation to the class 1 material that were not complied with.[420] Failure to comply with a link deletion notice will result in a civil penalty and the various enforcement actions as mentioned above. Another power vested in the OESC under the Online Safety Act is the ability to issue an app removal notice. Section 128 allows the OESC to issue an app removal notice which is a written notice to an app distribution service requiring the removal of an app that provides access to class 1 material within 24 hours or a timeframe specified by the OESC. As there is a potential that some intimate images may be classified as class 1 material, both of these notices may apply in the context of IBSA which may assist in the reduction of access to intimate images hosted overseas.

2.5.4 Overview of the key changes in the context of image-based sexual abuse

Overall, the Online Safety Act 2021 has brought about changes to the OESC processes and powers in relation to IBSA. These changes allow for the OESC to be more responsive to IBSA in an ever-changing technological environment. The key changes include:

- An expanded definition of intimate images to clearly include altered images, images depicting a person, and images of a person without their religious attire.
- The new power of the OESC to request the identity of an end user and provision of contact details from a service provider.

[419] ibid s 124.
[420] ibid s 124 (4).

- The ability to issue a service provider statement with the ability to name and shame non-compliant service providers.
- The reduced time frame to respond to a removal notice from 48 hours to 24 hours.
- The requirement of the OESC to provide an internal review process so to ensure due process.
- The ability to reduce the access to intimate images through link deletion notices and app removal notices.
- The ability to summon a person by written notice to appear before the OESC to produce documents or to answer questions or to provide documents or other information to the OESC relevant to the subject matter of the investigation.

2.6 Extracting the key needs of IBSA victims and identifying tools/mechanisms with the potential to address those needs from the Australian experience

Having reviewed the academic literature, it is clear that victims of IBSA have several needs that need to be addressed by law and policy. Based on the research conducted thus far, these needs can be categorised into six key categories of needs:

1. Constraining distribution of the image
2. Effective alternatives to constraining IBSA image
3. Adequately trained and resourced authorities
4. Prompt action
5. Empowerment
6. Confidentiality

While there may be overlaps and intersections between these categories at times, these categories provide a useful organising structure to consider how victim needs can be better centred in legislative and policy responses to IBSA. Furthermore, from its review of the Australian legislative and policy approach and academic literature, this thesis identifies eight tools/mechanisms that can be used to address the identified needs of IBSA victims. The identified tools/mechanisms are:

1. An independent specialist authority
2. An individual complaints mechanism
3. Removal orders
4. Orders reducing the visibility of IBSA material
5. Statutorily supported codes of practice

6. Educational campaigns
7. Civil avenues of redress
8. IBSA recognition as a criminal offence

These identified needs and tools/mechanisms form the basis of the framework from which this thesis assesses legislative and policy responses to IBSA in Australia and Ireland. This framework is victim-centred and is applied and reapplied throughout this thesis. The following sections will explain the various components of the victim-centred framework of this thesis which will subsequently be represented in a table.

2.6.1 Constraining distribution of the image

It is important to recognise that IBSA can cause harm in multiple ways and at different points in time. There is the 'initial harm' where an image is taken without consent or where an image taken with consent is subsequently shared in a manner not consented to. In addition, there is the 'additional/further harm' whereby an intimate image may be further shared or reposted online, downloaded, or resurfaced through search engine results. The literature has clearly identified a stated need of victims to have their image removed from the internet.[421]

Ideally a legal system should deter the commission of the initial harm of either taking images without consent or sharing an image taken with consent in a manner not consented to by the victim. Once that initial harm has occurred, however, the literature identifies a strong need for victims of IBSA to constrain the distribution of the image. This can include the deletion of an image from electronic devices or cloud storage, the removal of a specific posting of IBSA material from a website, or measures taken to prevent the reposting of an identified instance of IBSA online. Henry, Flynn, and Powell identify the removal of intimate images from 'internet sites or mobile phones' as one of the 'most pressing priorities' in providing an effective remedy for victims. [422] This finding is supported by further work where it is concluded that 'without exception, the key priority for victim-survivors in whatever jurisdiction is the removal or take-down of their images

[421]Erika Rackley, Clare McGlynn, Kelly Johnson, Nicola Henry, Nicola Gavey, Asher Flynn and Anastasia Powel, 'Seeking Justice and Redress for Victim-Survivors of Image-Based Sexual Abuse' (2021) 29 Feminist Legal Studies 317.
[422] Nicola Henry, Asher Flynn & Anastasia Powell, 'Policing Image-Based Sexual Abuse: Stakeholder Perspectives' (2018) 19 Police Practice and Research 577.

from wherever they have been posted'.[423] Similarly, Kitchen described the removal of the intimate images as 'one of the results victims most desire'.[424]

Bond and Tyrell explain while the original posting of the image may be removed, additional and further harm may persist when the image resurfaces or remains searchable through a search engine.

> Where the image(s) and video content are originally posted is not always the main issue in tackling the problem as, even though the image(s) or video(s) can be removed, they can remain searchable and, therefore, often still exist in search engines like Google. This is especially so if the image has been tagged or associated with a person's name.[425]

The challenge of relying on traditional criminal law approaches to address this need of victims is demonstrated by Cook who notes that 'the availability of a criminal sanction is of little practical value for a victim, since it does little to prevent further dissemination of the image'.[426] Rackley, McGlynn, Kelly, Johnston, Henry, Gavey, Flynn, and Powell also identified the need to constrain the distribution of the intimate image stating:

> The abuse is often ongoing, cumulative and relentless because the photographs or videos remain 'out there', constantly available to be shared online, viewed and rediscovered, with each new viewing or distribution a form of abuse.[427]

In sum, once the initial act of taking an image without consent or sharing a consensually taken image without consent has occurred, victims prioritise the constraining of the distribution of their image. Due to the nature of the internet, this is not a straightforward task to be completed on a single occasion but will often require ongoing review of some kind to remove – or even prevent – further distribution of the IBSA material. This is a pressing need of victims which must be considered in any response to IBSA.

2.6.2 Effective alternatives to constraining IBSA images

The criminalisation of IBSA is a relatively new phenomenon and the adoption of such laws in Australia at the state and federal level represents important progress in recognising

[423]Erika Rackley, Clare McGlynn, Kelly Johnson, Nicola Henry, Nicola Gavey, Asher Flynn and Anastasia Powel, 'Seeking Justice and Redress for Victim-Survivors of Image-Based Sexual Abuse' (2021) 29 Feminist Legal Studies 317.
[424]Adrienne N. Kitchen, 'The Need to Criminalize Revenge Porn: How a Law Protecting Victims Can Avoid Running Afoul of the First Amendment' (2015) 90 Chicago-Kent Law Review
[425] Emma Bond and Katie Tyrrell, 'Understanding Revenge Pornography: A National Survey of Police Officers and Staff in England and Wales' (2018) 36 Journal of Interpersonal Violence 2171.
[426] D. Cook, 'Revenge pornography' (2015) 179 Criminal Law and Justice Weekly 152.
[427]Erika Rackley, Clare McGlynn, Kelly Johnson, Nicola Henry, Nicola Gavey, Asher Flynn and Anastasia Powel, 'Seeking Justice and Redress for Victim-Survivors of Image-Based Sexual Abuse' (2021) 29 Feminist Legal Studies 298.

the harm caused by IBSA. It has been recognised that such reforms are 'not enough to secure justice'.[428] There are particular challenges to the effective vindication of victim rights in the IBSA context. When reviewing a system from a victim-centred perspective, it is crucially important that the system takes account of the specific challenges of IBSA in order to be effective.

In light of the capacity for large scale instantaneous sharing of IBSA and the associated legal issues which occur across the jurisdictional boundaries over which data flows so readily, there are particular challenges to meeting the needs of victims of IBSA. Kim clearly identifies these challenges associated with the regulation of IBSA on the internet explaining how the harms are exacerbated due to the internet's capabilities stating:

> IBSA injuries are in a class by themselves because it is so easy to disseminate quickly and because it is almost impossible to stop the spread of these images or delete them from every website on which they appear. The images last indeterminately, and because websites are accessible internationally, the images can cause widespread reputational damage. Thus, there is no comparison to harm in the real world.[429]

Kitchen explains how the potential for the 'dozens or even hundreds of Web sites' to redistribute intimate images, makes it 'nearly impossible to remove them from the web'. [430] Franks further argues that while 'most victims want the offensive material removed', many 'almost never succeed in removing the images due to the sheer magnitude of dissemination'.[431] Kim supports this argument describing IBSA as 'unique' because of its 'widespread dissemination and resulting harms'.[432]

> Anyone with internet access can post revenge porn anonymously for free, and it affects private individuals in a considerably more public manner than was possible before the internet.[433]

Kitchen also highlights the challenge associated with the borderless internet in seeking practical solutions stating, 'jurisdiction is another potential issue, simply because of the

[428] Nicola Henry, Clare McGlynn, Asher Flynn, Kelly Johnson, Anastasia Powell and Adrian J. Scott, *Image-Based Sexual Abuse: A Study on the Causes and Consequences of Non-Consensual Nude or Sexual Imagery*, (Taylor & Francis Group, 2020).
[429] Nancy S. Kim, 'Web Site Proprietorship and Online Harassment' (2009) Utah Law Review.
[430] Adrienne N. Kitchen, 'The Need to Criminalize Revenge Porn: How a Law Protecting Victims Can Avoid Running Afoul of the First Amendment' (2015) 90 Chicago-Kent Law Review
[431] Mary Anne Franks, 'Why We Need a Federal Criminal Law Response to Revenge Porn' (Concurring Opinions, 15 February 2013).
[432] Nancy S. Kim, 'Web Site Proprietorship and Online Harassment' (2009) Utah Law Review.
[433] ibid.

ease of posting revenge porn from anywhere at any time'.[434] Franks further identifies the challenges in providing effective practical remedies for IBSA victims as 'it is difficult to identify and prove who the perpetrator is for legal proceedings because it is so easy to anonymously post and distribute revenge porn'.[435]

The removal of IBSA material and the constraining of its distribution has been identified as a priority need of victims. In view of the challenges detailed, the complete removal of IBSA material may not always be possible and as a result there is a need for practical alternative solutions and effective remedies. Interviews with representatives from the Australian Police conducted by Powell and Henry identified the need for alternative solutions where removal of the image or constraining of its distribution is unachievable in order to minimise the harm and further harm caused to victims. One interview candidate stated that you cannot 'erase' an intimate image while another identified that the image can 'never be retrieved' and that this can have a 'massive' negative effect on victims.[436] Henry and Flynn also identified that while victims may have removal success with the large social media sites, 'on the more "rogue" sites where humiliation, abuse, degradation, and objectification of women are not only supported but actively encouraged, such requests may simply be ignored'.[437]

In order to minimise the harm caused to victims and provide effective responses, there is a need for continual support even after the original image is removed from the identified location. Powell, Flynn, Scott, and Henry explain the need for 'recurring support and advice' for victims as they live with the 'ongoing fear that the images will re-emerge and continue to be re-shared'.[438] Removal of the image and any subsequent reposts of the image is key to achieve this need and remedy victims. However, where the ultimate solution of complete removal cannot be achieved, there is a need for an alternative solution in order to reduce the availability of the disseminated image.

2.6.3 Adequately trained and resourced authorities

[434] Adrienne N. Kitchen, 'The Need to Criminalize Revenge Porn: How a Law Protecting Victims Can Avoid Running Afoul of the First Amendment' (2015) 90 Chicago-Kent Law Review
[435] Mary Anne Franks, 'Why We Need a Federal Criminal Law Response to Revenge Porn' (Concurring Opinions, 15 February 2013).
[436] Anastasia Powell and Nicola Henry, 'Policing Technology-Facilitated Sexual Violence Against Adult Victims: Police and Service Sector Perspectives' (2018)28 Policing and Society 299.
[437] Nicola Henry and Asher Flynn, 'Image-Based Sexual Abuse: Online Distribution Channels and Illicit Communities of Support' (2019) 25 Violence against Women 1950.
[438] Anastasia Powell, Asher Flynn, Adrian J. Scott and Nicola Henry, 'Image-Based Sexual Abuse: An International Study of Victims and Perpetrators' (Summary Report, February 2020)12.

In order for victims to be effectively remedied Bond and Tyrell highlighted the 'urgent need for training across police forces to ensure that cases of revenge pornography are appropriately responded to, victims are safeguarded, and offenders brought to justice'.[439] Flynn and Henry also highlighted this need for the provision of effective resources for victims explaining that there are several factors hindering police from providing appropriate support and responses to victims of IBSA.[440] These included 'a lack of resources, evidentiary limitations, jurisdictional boundaries, victim-blaming, or harm minimization attitudes held by police, and an absence of training on IBSA laws or on appropriate responses to victims of IBSA'.[441] Powell and Henry also echoed this point stating that there is a 'need to extend the training and resources for police to respond more effectively to victims'.[442]

Powell and Henry noted the increasing demand for 'forensic services for analysis of electronic evidence and hardware' as some police authorities struggle with poor technological facilities and slow internet connection. [443] Victims need police to be sufficiently resourced to be able to provide an effective response and be equipped to conduct an adequate investigation.

Rackley, McGlynn, Kelly, Johnston, Henry, Gavey, Flynn, and Powell also identified how the lack of resourcing and expertise by Police greatly impact victim's ability to seek redress. As a result, victims need to be able to engage with a service that is equipped with effective 'technical and practical support'.[444] As simply put by Flynn and Henry:

> There is no value to criminal law if those tasked with implementing, enforcing, and promoting it lack the requisite knowledge and skills to do so.[445]

While it is essential that law enforcement authorities are adequately equipped, Rackley, McGlynn, Johnston, Henry, Gavey, Flynn, and Powell note that victims need an

[439] Emma Bond and Katie Tyrrell, 'Understanding Revenge Pornography: A National Survey of Police Officers and Staff in England and Wales' (2018) 36 Journal of Interpersonal Violence 2166.
[440] Asher Flynn and Nicola Henry, 'Image-Based Sexual Abuse: An Australian Reflection' (2019) Women and Criminal Justice 322.
[441] ibid.
[442] Anastasia Powell and Nicola Henry, 'Policing Technology-Facilitated Sexual Violence Against Adult Victims: Police and Service Sector Perspectives' (2018)28 Policing and Society 304.
[443] Anastasia Powell and Nicola Henry, 'Policing Technology-Facilitated Sexual Violence Against Adult Victims: Police and Service Sector Perspectives' (2018)28 Policing and Society 302.
[444]Erika Rackley, Clare McGlynn, Kelly Johnson, Nicola Henry, Nicola Gavey, Asher Flynn and Anastasia Powel, 'Seeking Justice and Redress for Victim-Survivors of Image-Based Sexual Abuse' (2021) 29 Feminist Legal Studies 317.
[445] Asher Flynn and Nicola Henry, 'Image-Based Sexual Abuse: An Australian Reflection' (2019) Women and Criminal Justice.

independent authority in addition to law enforcement with expertise in online safety issues and a mandate to combat IBSA.[446] As they point out:

> What is also needed is a coherent strategy that combines proactive and reactive practical, legal and emotional support led by a public body accountable to Parliament for the implementation of this strategy.[447]

Briggs identified the importance of a 'standalone online safety entity' to address victim needs and further highlighted the importance of such an authority being adequately resourced to be able to give 'sharper focus to priority areas of online safety'.[448]

2.6.4 Prompt action

Henry, Flynn, and Powell identified the 'quick removal of non-consensual material'[449] as a key need of victims. Powell and Henry further identified that the element of 'time' is important for 'achieving justice for victims'.[450] Evans further supports this point by arguing that criminal and civil law actions fail to address the need of victims of IBSA 'to avail of a fast response'.[451] Evans also highlights the importance of prompt removal by stating that 'victims need an expedited remedy once publication or distribution has occurred'.[452]The literature clearly shows that victims require urgent action if the harms caused by IBSA are to be adequately mitigated. As the traditional systems of civil and criminal law struggle to provide the required immediacy, a victim-centred approach supports the establishment of a supplementary system to address the challenges of IBSA.

2.6.5 Empowerment

Henry, Flynn, and Powell identify the enabling of victims to report IBSA and the provision of 'access to support' as an 'important measure'[453] which assists in empowering victims. Henry, Flynn, and Powell also identified the need of empowering victims

---

[446]Erika Rackley, Clare McGlynn, Kelly Johnson, Nicola Henry, Nicola Gavey, Asher Flynn and Anastasia Powel, 'Seeking Justice and Redress for Victim-Survivors of Image-Based Sexual Abuse' (2021) 29 Feminist Legal Studies 318.
[447] ibid.
[448] Lynelle Briggs, *Report of the Statutory Review of the Enhancing Online Safety Act 2015 and the Review of Schedules 5 and 7 to the Broadcasting Services Act 1992 (Online Content Scheme)* October 2018.
[449] Nicola Henry, Asher Flynn & Anastasia Powell, 'Policing Image-Based Sexual Abuse: Stakeholder Perspectives' (2018) 19 Police Practice and Research 577.
[450] Anastasia Powell and Nicola Henry, 'Policing Technology-Facilitated Sexual Violence Against Adult Victims: Police and Service Sector Perspectives' (2018)28 Policing and Society 302.
[451] Michelle Evans, 'Regulating the Non-Consensual Sharing of Intimate Images (Revenge Pornography) via a Civil Penalty Regime: A Sex Equality Analysis' (2018) 44 Monash University Law Review 606.
[452] ibid 618.
[453] Nicola Henry, Asher Flynn & Anastasia Powell, 'Policing Image-Based Sexual Abuse: Stakeholder Perspectives' (2018) 19 Police Practice and Research 577.

through the need for 'increased support, advice, and information for a diversity of victims, to help them review the different options available, and to support them through what can be a highly stressful experience'.[454] Rackley, McGlynn, Kelly, Johnston, Henry, Gavey, Flynn, and Powell further identified the importance of empowering victim survivors explaining how victims need to be able to 'regain control' of their image within and beyond the criminal justice system.[455] The authors further explained this point stating that victims receive varying levels of redress by engaging with the criminal justice process but rather 'need to 'reclaim control' of their images, bodies, lives, relationships, careers, and physical and mental health. For many, this — rather than punishment of the perpetrator of the abuse — was their primary concern. [456] As a result, victims require empowerment to claim back control of their lives. Evans further argues the importance for victims of IBSA to feel empowered and highlights the need for them to be able to take control of their journey of redress and not rely on police to take action.[457]

> Criminal law does not seek to address the power imbalance between the victim and the perpetrator, because victims cannot seek a remedy themselves - they have to rely on police to investigate and to exercise their discretion to prosecute the perpetrator.[458]

2.6.6 Confidentiality

Franks identified one of the most significant harms suffered by victims of IBSA as the 'unwanted subjection to public scrutiny'.[459] Rackley, McGlynn, Kelly, Johnston, Henry, Gavey, Flynn, and Powell identified the importance of anonymity for victims when reporting IBSA to police as the report made may lead to criminal action being taken. As the victim may be identified in the criminal justice process, this can cause additional harm to the victim.[460]

---

[454] ibid 578.
[455] Erika Rackley, Clare McGlynn, Kelly Johnson, Nicola Henry, Nicola Gavey, Asher Flynn and Anastasia Powel, 'Seeking Justice and Redress for Victim-Survivors of Image-Based Sexual Abuse' (2021) 29 Feminist Legal Studies 312.
[456] ibid.
[457] Michelle Evans, 'Regulating the Non-Consensual Sharing of Intimate Images (Revenge Pornography) via a Civil Penalty Regime: A Sex Equality Analysis' (2018) 44 Monash University Law Review 606, 607.
[458] ibid.
[459] Mary Anne Franks, 'Unwilling Avatars: Idealism and Discrimination in Cyberspace' (2011) Columbia Journal of Gender and Law.
[460] Erika Rackley, Clare McGlynn, Kelly Johnson, Nicola Henry, Nicola Gavey, Asher Flynn and Anastasia Powel, 'Seeking Justice and Redress for Victim-Survivors of Image-Based Sexual Abuse' (2021) 29 Feminist Legal Studies 298; Clare McGlynn, Erika Rackley, Kelly Johnson, Nicola Henry, Asher Flynn, Anastasia Powell, Nicola Gavey and Adrian Scott, 'Shattering Lives and Myths: A Report on Image-Based Sexual Abuse.' (2019) Project Report. Durham University; University of Kent; Clare

> Anonymity is vital in order to increase police reports and successful prosecutions, as well as to protect complainants from further harm.[461]

The authors describe the lack of 'automatic anonymity for complainants' as 'egregious'.[462] The authors further explain that due to the lack of confidentiality afforded in the criminal justice process, this leads to a key barrier to victim-survivors reporting to the police.[463] Victims interviewed by the authors described the lack of anonymity provided when reporting to police as' ridiculous', 'crazy', 'outrageous', and 'such an obvious disaster'.[464] As a result the lack of confidentiality is a clear disincentive from approaching the police and supporting prosecutions.[465] Where laws criminalising IBSA do not provide for victim anonymity, supplementary mechanisms that allow for victims to object without the public reporting of their identity could have an important role to play in addressing the needs of victims.

2.7 Key tools/mechanisms

As mentioned previously, in the development of the victim-centred framework used in this thesis, the author also identifies key tools/mechanisms which can potentially address the identified needs of victims of IBSA. The key tools/mechanisms are explained below.

2.7.1 An independent specialist authority

Review of the literature identified an independent specialist authority with expertise in the area of IBSA as a key tool in addressing the needs of IBSA victims. Key Australian researchers identified this tool under various terms such as an 'office for online safety',[466]

McGlynn, 'Anonymity for Complainants of Image-Based Sexual Abuse: Focus on Harms to Victims, not Motives of Perpetrators' (2016) Centre for Gender Equal Media.

[461] Clare McGlynn, 'Anonymity for Complainants of Image-Based Sexual Abuse: Focus on Harms to Victims, not Motives of Perpetrators' (2016) Centre for Gender Equal Media.

[462] Erika Rackley, Clare McGlynn, Kelly Johnson, Nicola Henry, Nicola Gavey, Asher Flynn and Anastasia Powel, 'Seeking Justice and Redress for Victim-Survivors of Image-Based Sexual Abuse' (2021) 29 Feminist Legal Studies 298; Clare McGlynn, Erika Rackley, Kelly Johnson, Nicola Henry, Asher Flynn, Anastasia Powell, Nicola Gavey and Adrian Scott, 'Shattering Lives and Myths: A Report on Image-Based Sexual Abuse.' (2019) Project Report. Durham University; University of Kent; Clare McGlynn, 'Anonymity for Complainants of Image-Based Sexual Abuse: Focus on Harms to Victims, not Motives of Perpetrators' (2016) Centre for Gender Equal Media.

[463] ibid.

[464] Erika Rackley, Clare McGlynn, Kelly Johnson, Nicola Henry, Nicola Gavey, Asher Flynn and Anastasia Powel, 'Seeking Justice and Redress for Victim-Survivors of Image-Based Sexual Abuse' (2021) 29 Feminist Legal Studies 298.

[465] Erika Rackley, Clare McGlynn, Kelly Johnson, Nicola Henry, Nicola Gavey, Asher Flynn and Anastasia Powel, 'Seeking Justice and Redress for Victim-Survivors of Image-Based Sexual Abuse' (2021) 29 Feminist Legal Studies 298.

[466] ibid, 318.

'statutory officer'[467], and 'a targeted reporting mechanism'.[468] Rackley supports the establishment of an independent statutory body explaining it provides a 'single point of contact for victim-survivors' and removes the 'time-consuming and at times disorientating process of moving between organisations' when seeking help.[469]

Drawing from the Australian experience, Rackley, McGlynn, Johnston, Henry, Gavey, Flynn, and Powell note the importance recommended the establishment of a national, Government and/or industry-funded body that would provide 'direct help and support' for victim-survivors with an educative focus on 'individuals protecting themselves' in the United Kingdom.[470] The authors note that an independent specialist body can address victim needs for 'empowerment and effective solutions'. [471]

2.7.2 Individual complaints mechanism

Review of the literature particularly identified an individual complaints mechanism administered by an independent specialist authority as essential in addressing the identified needs of IBSA victims. Key Australian researchers identified 'image takedown assistance' and a 'complaints portal' as necessary to adequately address the needs of victims.

For example, in 2018, Henry, Flynn and Powell supported the expansion of the concept of a 'complaints portal' (which was previously successful in the cyberbullying context) to the IBSA context to enable IBSA victims to report their image.[472] Henry, Powell and Flynn identify the ability for victims to make a complaint directly to a speciality authority as essential for addressing the needs of victims.[473]

---

[467] Michelle Evans, 'Regulating the Non-Consensual Sharing of Intimate Images (Revenge Pornography) via a Civil Penalty Regime: A Sex Equality Analysis' (2018) 44 Monash University Law Review 618.
[468] Henry, Powell and Flynn, 'Not Just 'Revenge Pornography': Australians Experience of Image-Based Abuse' (2017) Summary Report.
[469] Ericka Rackley, 'Seeking Justice for Victim-Survivors of Image-Based Sexual Abuse' in Nicola Henry, Clare McGlynn, Asher Flynn, Kelly Johnson, Anastasia Powell, and Adrian J. Scott (eds) *Image-Based Sexual Abuse : A Study on the Causes and Consequences of Non-Consensual Nude or Sexual Imagery* (Taylor & Francis Group 2020).
[470] Erika Rackley, Clare McGlynn, Kelly Johnson, Nicola Henry, Nicola Gavey, Asher Flynn and Anastasia Powel, 'Seeking Justice and Redress for Victim-Survivors of Image-Based Sexual Abuse' (2021) 29 Feminist Legal Studies 318.
[471] ibid.
[472] Nicola Henry, Asher Flynn & Anastasia Powell, 'Policing Image-Based Sexual Abuse: Stakeholder Perspectives' (2018) 19 Police Practice and Research 577.
[473] Nicola Henry, Anastasia Powell, and Asher Flynn, 'Not Just 'Revenge Pornography': Australians Experience of Image-Based Abuse' (2017) Summary Report.

> ‘Providing a single-entry point for victims of image-based abuse will assist in providing victims with the remedies that they need, such as advice and counselling, and most importantly, takedown of non-consensual imagery’.[474]

Furthermore, Evans identifies the importance of an individual complaints mechanism to be able to act ‘expeditiously’ after receiving a complaint from a victim.[475] Farrell, Shackleton, Agnew, Hopkins, and Power explained that a regulatory approach such as a complaints mechanism ‘offers a quick, low-cost method for mitigating harm from IBSA’ and also represents ‘a welcome alternative’ to other more traditional approaches such as criminal or civil remedies.[476]

2.7.3 Removal orders

As explained in section 2.6.1 the primary concern for victims of IBSA is often the removal of the image from the internet as soon as possible. While the harms experienced by the disseminated images exist from the moment of first non-consensual taking or distribution, the continuing harms of the images remaining available online can be minimised or reduced by preventing further distribution. The most obvious way to do this is to require the person who uploaded the image to remove it from where it can be accessed.[477] However, in some cases the perpetrator is not willing to comply with a request – or even an order – for removal. In addition, where the image has been covertly taken, obtained as a result of hacking, or simply shared beyond a traceable social circle, the victim may not know the identity of the poster and additional challenges arise unless the identity can be uncovered in some way. As a result, victims may seek to request that the host platform remove the image.

> Where individual perpetrators cannot be identified, there are important questions around the accountability of websites which are hosting illegal content.[478]

Rackley notes the desire of victims ‘to hold the online platforms accountable – and in particular, for them to take responsibility’[479] which can be achieved in the Australian

[474] ibid.
[475] Michelle Evans, ‘Regulating the Non-Consensual Sharing of Intimate Images (Revenge Pornography) via a Civil Penalty Regime: A Sex Equality Analysis’ (2018) 44 Monash University Law Review 618.
[476] Anne-Maree Farrell, Nicole Shackleton, Elizabeth Agnew, Samantha Hopkins and Jennifer Power, ‘Regulating Tech-Sex and Managing Image-Based Sexual Abuse: An Australian Perspective’ (2022) Information & Communications Technology Law.
[477] Aislinn O’Connell and Ksenia Bakina, ‘Using IP Rights to Protect Human Rights: Copyright for ‘Revenge Porn’ Removal’ (2020) 40 Legal Studies.
[478] Ericka Rackley, ‘Seeking Justice for Victim-Survivors of Image-Based Sexual Abuse’ in Nicola Henry, Clare McGlynn, Asher Flynn, Kelly Johnson, Anastasia Powell, and Adrian J. Scott (eds) *Image-Based Sexual Abuse: A Study on the Causes and Consequences of Non-Consensual Nude or Sexual Imagery* (Taylor & Francis Group 2020).
[479] ibid.

system for example through a removal order issued directly to the platform. O'Connell and Bakina have noted that intermediaries can be reluctant to comply with such removal requests 'without legal accountability attached'.[480]

Consequently, while individual complaints mechanisms are a valuable tool for reporting IBSA occurrences, such mechanisms are particularly effective where they are attached to the ability to take action when voluntary compliance requests to remove material are not met. Henry, Flynn, and Powell highlight the importance of removal notices that are supported with statutory power as a valuable tool in addressing victims needs for removal and the regaining of control of their image.

> The study also recommends the introduction of legislation that empowers courts and/or independent government agencies to compel individuals to take all reasonable steps to remove, delete or destroy nonconsensual nude or sexual images, with further criminal or civil penalties for noncompliance.[481]

2.7.4 Orders reducing visibility of IBSA material

While the removal of the IBSA material is priority, many victims 'almost never succeed in removing the images due to the sheer magnitude of dissemination'[482] and the jurisdictional issues associated with the internet. As a result, where removal orders are unsuccessful, there is a necessity for tools reducing the visibility of the content by removing it from search engine results or by blocking access to the hosting page in the jurisdiction of the victim so to reduce the harms experienced by victims. In addition, where a removal order is unenforceable due to the image being hosted overseas, an order reducing visibility of the IBSA material offers an alternative solution.

2.7.5 Statutorily supported codes of practice

Flynn and Henry call for statutorily supported codes of conduct agreed collaboratively with industry to encourage intermediaries to develop victim-centred practices as a key tool to address victim's needs.

> Other measures should include those focused on corporate and organizational "bystanders," including government and community representatives working collaboratively with Internet, website, social media, and other service providers in order to promote service agreements and community codes of conduct that

[480] Aislinn O'Connell and Ksenia Bakina, 'Using IP Rights to Protect Human Rights: Copyright for 'Revenge Porn' Removal' (2020) 40 Legal Studies.
[481] Nicola Henry, Asher Flynn and Anastasia Powell, 'Image-based sexual abuse: Victims and perpetrators' (2019) 572 Trends & Issues in Crime and Criminal Justice 15.
[482] Mary Anne Franks, 'Why We Need a Federal Criminal Law Response to Revenge Porn' (Concurring Opinions, 15 February 2013).

> include clear statements regarding the unacceptability of IBSA and appropriate consequences for an individual's violation of such terms of service/ codes of conduct.[483]

Henry, Flynn, and Powell further note that for the tool of codes of practice to be effective they should not be voluntary but rather there be a legal obligation imposed on internet service providers, search engine operators and social media companies to have clear polices for the removal of intimate images from their platforms.[484]

> There should be a review of the regulatory frameworks that impose legal obligations on internet service providers, search engine operators and social media companies to screen content, have clear takedown (removal) policies, and take responsibility for removing images within reasonable time frames.[485]

Farrell, Shackleton, Agnew, Hopkins, and Power also highlight the value in the development of 'core principles setting out expectations regarding online safety'[486] so to ensure platform reporting avenues and takedown procedures are meeting victim needs.

2.7.6 Educational campaigns

While remediation strategies are essential in addressing the needs of IBSA victims, 'preventative strategies' are also an 'important aspect of any regulatory approach'.[487] As a result, a 'multifaceted' response is essential.[488] Farrell, Shackleton, Agnew, Hopkins, and Power support the importance of 'educational and awareness raising activities' that promote online safety including online safety related to IBSA.[489] Henry and Flynn support this idea explaining the importance of multiple tools/mechanisms in responding to IBSA with the law 'only being one part of the solution to IBSA' when providing redress.[490] In addition to legal redress, victims need a 'measure' which is designed to provide 'support, advice and assistance' and in addition 'educate the broader public'. [491]

---

[483] Asher Flynn and Nicola Henry, 'Image-Based Sexual Abuse: An Australian Reflection' (2019) Women and Criminal Justice 322.
[484] Nicola Henry, Asher Flynn and Anastasia Powell, 'Image-based sexual abuse: Victims and perpetrators' (2019) 572 Trends & Issues in Crime and Criminal Justice 15.
[485] ibid.
[486] Anne-Maree Farrell, Nicole Shackleton, Elizabeth Agnew, Samantha Hopkins and Jennifer Power, 'Regulating Tech-Sex and Managing Image-Based Sexual Abuse: An Australian Perspective' (2022) Information & Communications Technology Law.
[487] ibid.
[488] Asher Flynn, Elena Cama and Adrian J Scott, 'Preventing Image-Based Abuse in Australia: The Role of Bystanders' Report to the Criminology Research Advisory Council Grant: CRG 02/18–19 (August 2022).
[489] Anne-Maree Farrell, Nicole Shackleton, Elizabeth Agnew, Samantha Hopkins and Jennifer Power, 'Regulating Tech-Sex and Managing Image-Based Sexual Abuse: An Australian Perspective' (2022) Information & Communications Technology Law.
[490] Nicola Henry and Asher Flynn, 'Image-Based Sexual Abuse: Online Distribution Channels and Illicit Communities of Support' (2019) 25 Violence against Women 1950.
[491] ibid.

Flynn, Cama, and Scott also highlight this view explaining how legal responses must be accompanied with 'non-legal options and education and prevention messaging in order to be effective and provide avenues for justice beyond the legal realm'.[492]

Flynn and Henry identified the importance of educational campaigns to address in particular victim blaming attitudes and help remove the barriers victims face when reporting their case.[493]

It is also vital that changes in the law are accompanied by education campaigns that raise awareness of the causes, harms, and impacts of IBSA, and that promote proactive and safe bystander interventions.[494]

McGlynn, Rackley, Johnson, Henry, Flynn, Powell, Gavey, and Scott explain further the importance of educational campaigns to address the needs of IBSA victims. In particular, the authors highlight the importance of a Government Office 'to provide specialist advice, assistance and support for victim-survivors, as well as focussing on prevention through education'.[495] Of particular relevance is 'comprehensive police training and guidance on responding to IBSA' and 'Government funded education and prevention campaigns to challenge attitudes and motivations driving IBSA'.[496] Raising awareness and educating people about the harms of IBSA abuse is fundamental, so that IBSA behaviours are not 'normalised' and so that the victims do not feel that they just need to 'laugh at a prank' or 'suffer silently'.[497] Echoing this view, Flynn, Cama, and Scott highlight the importance of education in order to challenge 'victim blaming cultures within society' that can prevent victims from seeking assistance.[498]

Overall, as stated by Rackley, McGlynn , Johnson , Henry , Gavey, Flynn, and Powell, victims of IBSA have a 'desire for education as a form of justice',[499] as educational

[492] Asher Flynn, Elena Cama and Adrian J Scott, 'Preventing Image-Based Abuse in Australia: The Role of Bystanders' Report to the Criminology Research Advisory Council Grant: CRG 02/18–19 (August 2022).
[493] Asher Flynn and Nicola Henry, 'Image-Based Sexual Abuse: An Australian Reflection' (2019) Women and Criminal Justice 322.
[494] ibid.
[495] Clare McGlynn, Erika Rackley, Kelly Johnson, Nicola Henry, Asher Flynn, Anastasia Powell, Nicola Gavey and Adrian Scott, 'Shattering Lives and Myths: A Report on Image-Based Sexual Abuse.' (2019) Project Report. Durham University; University of Kent.
[496] ibid.
[497] Clare McGlynn, Erika Rackley, Kelly Johnson, Nicola Henry, Asher Flynn, Anastasia Powell, Nicola Gavey and Adrian Scott, 'Shattering Lives and Myths: A Report on Image-Based Sexual Abuse.' (2019) Project Report. Durham University; University of Kent.
[498] Asher Flynn, Elena Cama and Adrian J Scott, 'Preventing Image-Based Abuse in Australia: The Role of Bystanders' Report to the Criminology Research Advisory Council Grant: CRG 02/18–19 (August 2022).
[499] Erika Rackley, Clare McGlynn, Kelly Johnson, Nicola Henry, Nicola Gavey, Asher Flynn and Anastasia Powell, 'Seeking Justice and Redress for Victim-Survivors of Image-Based Sexual Abuse' (2021) 29 Feminist Law Studies.

campaigns reduce victim-blaming attitudes which results in a safer environment to report while also providing victims with clear guidance on their rights and potential avenues of redress. Simply stated:

> There are, in other words, many different ways of enabling a sense of justice, from securing consequences for the perpetrator, developing educational and prevention responses, and treating victim-survivors with dignity and affording them recognition of the harms experienced.[500]

2.7.7 Civil avenues of redress

Civil avenues of redress, including by means of injunctive relief, can be a potential tool for IBSA victims. Damages awards have been made in IBSA cases[501] and injunctions may be of assistance in restraining the dissemination of intimate images.

The importance of damages was highlighted in the recent case of *FGX v Stuart Gaunt* where Justice Thornton awarded the victim general damages of £60,000 and special damages of £37,041.61 for consequential financial losses. Justice Thornton identified that the 'impacts on the claimant are akin to the impacts of sexual assault…albeit that the abuse…is image based rather than physical' when justifying the award of general damages. Justice Thornton further recognised that the availability of the images on the internet and the possibility of the replication of the images elsewhere has led to severe injury to the victim which justified an award of damages. The award of damages enables the victim to seek professional help for the harms experienced and any future treatment needed (such as PTSD which was experienced by the victim in *FGX v Stuart Guant*). Furthermore, the award of damages can also assist victims in removing images from the internet. In *FGX v Stuart Guant*, Justice Thornton allocated £21,600 towards the cost of the removal of the images from the internet as part of the overall award of damages.

Evans argues that victims being threatened with exposure must have 'recourse to immediate relief to prevent such sharing or distribution from occurring'.[502] Evans supports the availability of preventative injunctive relief whereby victims seek immediate injunctive relief 'at first instance to protect victims until the initial investigation is

[500] Erika Rackley, Clare McGlynn, Kelly Johnson, Nicola Henry, Nicola Gavey, Asher Flynn and Anastasia Powell, 'Seeking Justice and Redress for Victim-Survivors of Image-Based Sexual Abuse' (2021) 29 Feminist Law Studies.
[501] *Wilson v Ferguson* [2015] WASC 15; FGX v Stuart Gaunt [2023] EWHC 419 (KB).
[502] Michelle Evans, 'Regulating the Non-Consensual Sharing of Intimate Images (Revenge Pornography) via a Civil Penalty Regime: A Sex Equality Analysis' (2018) 44 Monash University Law Review 615.

finalised'.[503] Evans argues that injunctive relief should be linked to prevention rather than solely enforcement as an injunction at the enforcement stage 'may be too late to prevent or contain the distribution of the image and to stop a victim from suffering substantial and irreparable harm'.[504] In the case Wilson v Ferguson, Justice Mitchell explained the importance of injunctive relief even after the image has been posted to avoid further reposting of the image.

> The past conduct of the defendant in publishing the images of the plaintiff gives rise to a reasonable apprehension that the conduct might be repeated.[505]

2.7.8 IBSA recognition as a criminal offence

Criminal law 'protects the public against harm by punishing harmful results of conduct'[506] and carries 'community condemnation'.[507] Criminal law 'incentivizes obedience to the law' with the threat of punishment deterring those who might engage in criminal activities.[508]

Given the pervasiveness and impacts of IBSA, governments around the world have introduced 'specifically crafted' criminal laws making IBSA a criminal offence.[509] In some countries, the criminal law is 'complex' and 'piecemeal', with separate laws covering the distribution of sexual images, voyeurism and upskirting[510] while in other jurisdictions, the laws are more 'comprehensive, capturing the complexity and harms' of IBSA.[511] Kitchen describes a targeted law criminalising IBSA as a 'vital' deterrent as the dissemination of IBSA becomes 'increasingly easy'.[512] Rackley, McGlynn, Johnson,

[503] ibid.
[504] ibid.
[505] Wilson v Ferguson [2015] WASC 15.
[506] Wayne R. LaFave, *Substantive Criminal Law* (3rd edn, Thomas Reuters 2013).
[507] Henry M. Hart Jr., 'The Aims of the Criminal Law' (1958) 23 Law & Contemporary Problems.
[508] Marcelo Ferrante, 'Deterrence and Crime Results' (2007)10 New Criminal Law Review.
[509] Nicola Henry, Clare McGlynn, Asher Flynn, Kelly Johnson, Anastasia Powell and Adrian J. Scott, *Image-Based Sexual Abuse: A Study on the Causes and Consequences of Non-Consensual Nude or Sexual Imagery*, (Taylor & Francis Group, 2020)135.
[510] Clare McGlynn, Erika Rackley, Kelly Johnson, Nicola Henry, Asher Flynn, Anastasia Powell, Nicola Gavey & Adrian Scott, 'Shattering lives and myths: A report on image-based sexual abuse' (2019) *Project Report. Durham University; University of Kent*.
[511] Nicola Henry, Clare McGlynn, Asher Flynn, Kelly Johnson, Anastasia Powell and Adrian J. Scott, *Image-Based Sexual Abuse: A Study on the Causes and Consequences of Non-Consensual Nude or Sexual Imagery*, (Taylor & Francis Group, 2020)135.
[512] Adrienne N. Kitchen, 'The Need to Criminalize Revenge Porn: How a Law Protecting Victims Can Avoid Running Afoul of the First Amendment' (2015) 90 Chicago-Kent Law Review.

Henry, Gavey, Flynn, and Powell argue that the criminalisation of IBSA provides 'recognition and redress' to victims.[513]

2.8 Assessing how the identified tools/mechanisms can potentially address the needs of IBSA victims

The table below demonstrates the relationship between the identified categories of needs of IBSA victims and the identified tools/mechanisms with potential to address those needs. This table is informed by research by key authors in the field of IBSA as discussed in sections 2.6 and 2.7, and the desk-based research conducted in this chapter on the Australian response to IBSA. The below table will be used throughout this thesis and refined in response to research discussed in subsequent chapters.[514]

Identified tools/mechanisms that address the needs of victims of IBSA

Identified needs of victims of IBSA	*Independent specialist authority*	*Individual complaints mechanism*	*Removal orders*	*Orders reducing visibility of IBSA material*	*Statutorily supported codes of practice*	*Educational campaigns*	*Civil avenues of redress*	*IBSA recognition as a criminal offence*
Constraining distribution of the image	+	+	+		+		+	+
Effective alternatives to constraining IBSA images	+	+		+				
Adequately trained and resourced authorities	+					+		
Prompt action	+	+	+	+	+			
Empowerment	+	+				+		+
Confidentiality	+	+						

Figure 6 Framework table illustrating the relationship between the needs of IBSA victims and the potential tools/mechanisms as informed by the Australian experience

The top row of the table sets out the tools/mechanisms identified as having the potential to at least partially address the needs of victims of IBSA. The first column sets out the six

[513] Erika Rackley, Clare McGlynn, Kelly Johnson, Nicola Henry, Nicola Gavey, Asher Flynn and Anastasia Powell, 'Seeking Justice and Redress for Victim-Survivors of Image-Based Sexual Abuse' (2021) 29 Feminist Legal Studies 317.
[514] See sections 3.10, 3.10.7, 4.4, 4.4.1, 5.6, 5.6.7.

identified categories of key needs of IBSA. The various plus symbols '+' are used to illustrate which mechanisms have the potential to address – at least in part – which need. For example, the first '+' symbol marked beside the need of 'constraining distribution of the image' and under 'independent specialist authority' indicates that the mechanism of an independent specialist authority has the potential to address the need to constrain the distribution of IBSA material. The following sections provide an overview of how the various tools/mechanisms displayed in the top row connect and address the various needs displayed in the first left column.

2.8.1 Tool/mechanisms addressing the need of constraining distribution of the image

The identified victim need of constraining the distribution of IBSA material is most directly addressed by removal orders. In addition, five of the remaining seven identified tools/mechanisms[515] can also play a supportive role in addressing this key need.

The provision of an independent specialist authority with a mandate to ensure online safety provides victims with an avenue for redress which is equipped with specific expertise to address online safety issues. In the Australian context, this includes the ability to constrain the distribution of intimate images. An independent specialist body can address victim's need to remove their intimate image by providing information on how to seek removal and options available to victims. Furthermore, such an authority can provide removal assistance by utilising its connections which may be established with key platforms. In the Australian context the OESC provides many useful resources to IBSA victims including the provision of online information, educational tools and programmes which can assist with image removal and the regaining of control of an image.[516] The OESC website has been described as a 'focal point for online safety issues'[517] and a 'trusted portal' for access to 'high quality'[518] online safety resources which include image removal. As discussed in section 2.4.1, the OESC website specifically addresses victim's need to constrain the distribution of intimate images by

[515] Namely: An independent specialist authority, an individual complaints mechanism, statutorily supported codes of practice, civil avenues of redress, and recognition of IBSA as a criminal offence.
[516] Australian Government Department of Communications and the Arts, Review of the Enhancing Online Safety Act 2015 and the Online Content Scheme – discussion (June 2018) 4.
[517] Amanda Third, 'Submission to the Review of the Enhancing Online Safety Act 2015 and the Online Content Scheme' (2018) 2.
[518] ibid.

providing useful information on 'how to report intimate images to eSafety',[519] 'how to remove intimate images',[520] 'how to deal with sexting'[521] and 'how to deal with sextortion'.[522] Finally, and perhaps most significantly, an independent specialist authority with the authority to compel the removal of IBSA can play a direct and powerful role in addressing the needs of victims to constrain the distribution of IBSA material. As discussed above, the Australian OESC has significant powers to enforce a compliance notice including through an injunction, enforceable undertaking, or a civil penalty.

While IBSA material may be removed on the initiative of a platform or a government authority, it is clear that victims have the clearest interest and incentive to have such material taken down. This underlines the importance of an individual complaints mechanism in supporting the constraining of IBSA material distribution. An individual complaints mechanism administered through an independent specialist authority, in particular, provides a direct avenue to report images in a less invasive, cost effective, and expeditious manner compared to other traditional avenues of redress.[523] The IBA portal administered by the OESC as discussed in section 2.4.4 addresses the need of IBSA victims to have their intimate images removed by informally requesting internet service providers to remove the reported intimate image voluntarily. The IBA portal has been successful in addressing victims needs to constrain the distribution of their images as images requested for removal were removed in 90% of cases by the OESC through the IBA portal.[524]

While individual complaints mechanisms such as the IBA portal are a valuable tool for reporting IBSA occurrences, such mechanisms are particularly effective where they are attached to the ability to take action when voluntary compliance requests to remove material are not met. As a result, the mechanism of removal orders that are supported by

[519] Office of the eSafety Commissioner, 'How to report IBSA' < https://www.esafety.gov.au/report/image-based-abuse> accessed 15 August 2020.
[520] Office of the eSafety Commissioner, 'Get help to remove images and video' <https://www.esafety.gov.au/key-issues/image-based-abuse/take-action/get-help-remove-images-video> accessed 15 August 2020.
[521] Office of the eSafety Commissioner, 'Sending nudes and sexting' < https://www.esafety.gov.au/key-issues/staying-safe/sending-nudes-sexting> accessed 15 August 2020.
[522] Office of the eSafety Commissioner, 'Deal with sextortion' < https://www.esafety.gov.au/key-issues/image-based-abuse/take-action/deal-with-sextortion> accessed 15 August 2020.
[523] Nicola Henry, Asher Flynn & Anastasia Powell, 'Policing Image-Based Sexual Abuse: Stakeholder Perspectives' (2018) 19 Police Practice and Research 577; Michelle Evans, 'Regulating the Non-Consensual Sharing of Intimate Images (Revenge Pornography) via a Civil Penalty Regime: A Sex Equality Analysis' (2018) 44 Monash University Law Review 618.
[524] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2020/21, 215.

statutory force are a valuable tool in addressing victim needs for removal and the regaining of control of their image. In the Australian context, where the IBA portal fails to secure removal of a requested image on a voluntary basis, the OESC can issue various compliance notices including service provider notifications[525] (whereby the OESC can notify an online service provider that they are hosting an intimate image that was reported or objected to and to remove the image) or a removal notice[526] to an end user who posted an intimate image. Failure to comply with such notices can result in various enforcement actions including an injunction, enforceable undertaking, or a civil penalty by the OESC following a court order.

While an order to remove an intimate image once posted is important, there is also a need for a tool to address the need of victims to constrain the dissemination of IBSA material following a threat or subsequent reposting of the image. The Australian context addresses this need by empowering the OESC with remedial directions which allows the OESC to issues a direction to prohibit a person threatening to post an intimate image from carrying out the threat. Furthermore, in order to be truly effective, removal orders must be supported by real penalties. In the Australian context, the civil penalty regime under the Online Safety Act 2021 allows the OESC to impose a monetary fine for non-compliance with a compliance notice and/or issue an injunction to compel compliance. The availability of such actions addresses the needs of victims to constrain the distribution of their image as these actions facilitate the removal of intimate images and the deterrence of future postings.

The identified need to contain the distribution of the image may also be addressed through the use of codes of practice. The encouragement of platforms to adopt codes of practice that provide for the removal of IBSA material has significant value for victims of IBSA. Such codes of practice – whether industry or government led – should provide for the establishment of transparent processes and reporting tools to facilitate effective and efficient takedown procedures. Codes of practice can be incorporated into platform terms of service and give notice to users of the platform of the processes available and rules applicable. While codes of practice have traditionally been industry led and often entirely voluntary in nature, statutorily supported codes of practice have the potential to be more effective in practice. The Australian Online Safety Act 2021 allows for the Minister for Communications to set 'Basic Online Safety Expectations' for social media services,

[525] Online Safety Act 2021, s 85.
[526] Online Safety Act 2021, s 77.

relevant electronic services, and designated internet services, outlining the fundamental safety practices expected of service providers, through a legislative instrument called a determination. The Online Safety (Basic Online Safety Expectations) Determination 2022 was registered on 23 January 2022. The key aim of the Basic Online Safety Expectations is to ensure service providers take reasonable steps to keep Australians safe online[527] and minimise the provision of certain identified material including 'a non-consensual intimate image of a person'.[528] While the expectations are not enforceable, the OESC has the power to require online service providers to report on how they are meeting any or all of the expectations,[529] require the service provider to respond to a reporting notice whereby failure to do so can result in civil penalties,[530] and the power to issue statements to provider(s) about compliance and non-compliance with the expectations and publish such statements.[531] This should provide some additional incentive to have effective platform policies supporting the removal of IBSA.

Civil avenues of redress, in particular damages, may be of assistance in restraining the dissemination of intimate images as the award of damages to victims can be put towards the cost of seeking assistance in removing of the intimate image and its subsequent replications.

The recognition of IBSA as a criminal offence may address victims needs to constrain the distribution of their image as criminalising IBSA and attached criminal sanctions to such behaviour deters potential threats being executed or reposting of an image following the original posting. This allows victims to regain an element of control over their intimate image and constrain its distribution in the first instance or further reposting once already posted. Within Australia, legislation recognising IBSA as a criminal offence has been introduced at the federal level under section 474.17(A) of the Criminal Code Act 1995 as amended by the Enhancing Online Safety Act (Non-Consensual Sharing of Intimate Images) Act 2018. In addition, all eight states/territories have enacted criminal laws recognising IBSA as a criminal offence with the exception of Tasmania which lacks a targeted law as discussed in section 2.2. The criminalisation of IBSA both at the state/territory and federal levels allows victims to constrain the distribution of their image

[527] The Online Safety (Basic Online Safety Expectations) Determination 2022, Expectation 6.
[528] The Online Safety (Basic Online Safety Expectations) Determination 2022, Expectation 11 (c).
[529] Basic Online Safety Expectations, Regulatory Guidance July 2022.
[530] Basic Online Safety Expectations, Regulatory Guidance July 2022.
[531] ibid.

by reporting it to police for removal assistance and the impact of the presence of the law assists in discouraging dissemination and reposting.

2.8.2 Tools/mechanisms addressing the need for effective alternatives to constraining IBSA material

The identified need for effective alternatives to constraining IBSA material can be addressed through three of the noted tools/mechanisms in the developed framework as follows: an independent specialist authority, individual complaints mechanism, and orders reducing visibility of IBSA material.

While the removal of IBSA material and the constraining of its distribution has been identified as a priority need of victims, the complete removal of IBSA material may not always be possible and as a result the need for practical alternative solutions and effective remedies was identified. Alternative solutions can include 'recurring support and advice' for victims as they live with the 'ongoing fear that the images will re-emerge and continue to be re-shared'[532] and solutions to reduce the visibility of the image on the internet.

The provision of an independent specialist authority can address this need as such a body can act as a 'one stop shop' for victims in need of support. Where removal cannot be achieved such a body can link victims with support services to help victims cope with their traumatic experience. In the Australian context the OESC provides support service through a webpage called eSafetyWomen which provides support to IBSA victims providing information about dealing with IBSA as well as an interactive 'check-up' testing knowledge about online safety and security.[533]

Due to the manner in which information is frequently accessed on the internet, a vitally important support where fully constraining the distribution of IBSA material is impossible is to have a system whereby search engines can be requested to de-index content. In the Australian context, the OESC can request search engines to voluntarily de-index access to an image that was reported through the IBA portal which failed to be removed following a removal notice.

Additional steps to reduce the visibility of the IBSA material can further support the needs of victims. Within Australia, the provision of link deletion notices[534] and app removal

[532] Anastasia Powell, Asher Flynn, Adrian J. Scott and Nicola Henry, 'Image-Based Sexual Abuse: An International Study of Victims and Perpetrators' (Summary Report, February 2020)12.
[533] Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2016/17, 121.
[534] Online Safety Act 2021, s 124.

notices[535] in the Online Safety Act 2021 to direct a search engine provider or an app store to remove a link or app which provides access to a reported intimate image particularly in cases where the content is hosted overseas, ensures reduced visibility of the intimate image. This addresses victim's need for an effective alternative solution by reducing the visibility of the content where removal is impossible.

2.8.3 Tools/mechanisms addressing the need for adequately trained and resourced authorities

The research demonstrates how victim needs have often been left unmet by under-trained and under-resourced authorities. Two identified tools/mechanisms with the potential to address this need are the establishment of an independent specialist authority and educational campaigns.

A trained and resourced specialist authority with a mandate to support victims of IBSA is a vital mechanism in the response to address the needs of victims of IBSA. The OESC meets the needs of victims for an adequately trained and resourced authority.

In addition to this, an independent specialist authority acts as a key point of contact for other organisations to liaise with to obtain specialist knowledge and use of resources. In the Australian context, the OESC administers a wide range of educational resources to key stakeholders in the field of online safety including IBSA. It is a 'trusted portal' for access to 'high quality' online safety resources. The OESC is focused on providing 'nationally coordinated online safety education' through various platforms and resources.[180] These resources support various groups of people including law enforcement. For example, the OESC provides virtual classroom training sessions to frontline workers providing knowledge and expertise to enable frontline workers such as the police to more effectively assist victims.

Educational campaigns can also assist in addressing the need of victims for adequately trained and resourced authorities. Educational campaigns can change attitudes and in particular reduce victim-blaming. They can also inform authorities – including police – of the harms of IBSA and its prevalence. In the Australian context, Internet safety campaigns – such as the 'ThinkUKnow' campaign and the New South Wales' 'Safe Sexting: No Such Thing' campaign – can assist in developing knowledge and understanding around IBSA.

[535] ibid s 128.

2.8.4 Tools/mechanisms addressing the need for prompt action

Due to the speed and magnitude at which IBSA can spread and the harms associated, victims require prompt action in order to minimise that harm. Five of the identified tools/mechanisms can assist in addressing this need including an independent specialist authority, an individual complaints mechanism, removal orders, orders reducing visibility of IBSA material, and codes of practice.

An independent specialist authority provides victims with a 'one stop shop' for information and guidance. Without this direct avenue to support, victims may have to research their options for redress which can often take time. Often such an authority can respond quicker than law enforcement as such an authority has a specific purpose of dealing with online issues such as IBSA and therefore have a more experienced and tailored workforce. For example, the OESC provides 'urgent' assistance to victims of online issues.[536]

An individual complaints mechanism can also provide prompt action as victims can report their image immediately upon awareness. The OESC IBA portal allows victims to report their image online from the comfort of their own home. This fast-track avenue of reporting compared to traditional reporting to police is less time consuming as there is no waiting time for report making and legal administrative procedures.

Furthermore, the provision of removal orders and orders reducing the visibility of IBSA material are also time sensitive as compared to traditional civil and criminal avenues of redress. A removal order and an order reducing the visibility of IBSA material whether given on an informal basis by a specialist authority or a formal basis following a court order attaches a time frame upon which the order/request has to be achieved. In the Australian context, compliance notices must be complied with within a 24-hour period.

Finally, the need for prompt action can also be supported through the development and adoption of codes of practice. In particular, the provision of statutorily supported codes can help to ensure the platform procedures and policies meet an effective standard. Codes of practice can require platforms to institute reporting systems to deal with IBSA material in a specified time frame. As platforms have the authority and technical ability to govern their own online space in accordance with their terms of service, platform takedown is

[536] Amanda Third, 'Submission to the Review of the Enhancing Online Safety Act 2015 and the Online Content Scheme' (2018) 2.

the speediest form of removal available. Accordingly, the development and adoption of codes of practice requiring consistent and transparent procedures supports victim access to the most direct and efficient route to image takedown.

2.8.5 Tools/mechanisms addressing the need for empowerment

As displayed in the table, the identified need for empowerment can be addressed by four of the identified tools/mechanisms, namely: an independent specialist authority, an individual complaints mechanism, educational campaigns, and IBSA recognition as a criminal offence.

An independent specialist authority empowers victims by providing support, advice, and guidance enabling victims to regain control of their lives. The Australian OESC provides this support through educational tools, resources, and the eSafetyWomen platform. The use of such services equips victims with options allowing them to make informed decisions on what avenue of redress is most suitable for their experience.

An individual complaints mechanism empowers victims as victims can make their own report directly without assistance from law enforcement or other third parties. The IBA portal allows victims to report their image directly to the OESC providing victims with a direct avenue of redress. Studies show that victims often feel alienated and disempowered by interactions with the traditional criminal justice system and the intention is that interactions with authorities like the OESC and their complaints mechanisms have the opposite effect.

Educational campaigns educate the broader public,[537] provide preventive messaging, [538] inform victims of their redress options, and reduce victim blaming attitudes thus removing the barriers victims face when reporting their cases.[539] Victims become more empowered as they are educated in the options available to them and also can seek redress without fear of judgement or blame.

Similarly, the recognition of IBSA as a criminal offence empowers victims by clearly identifying IBSA as a wrong that is not accepted by society.

---

[537] Nicola Henry and Asher Flynn, 'Image-Based Sexual Abuse: Online Distribution Channels and Illicit Communities of Support' (2019) 25 Violence against Women 1950.
[538] Asher Flynn, Elena Cama and Adrian J Scott, 'Preventing Image-Based Abuse in Australia: The Role of Bystanders' Report to the Criminology Research Advisory Council Grant: CRG 02/18–19 (August 2022).
[539] Asher Flynn and Nicola Henry, 'Image-Based Sexual Abuse: An Australian Reflection' (2019) Women and Criminal Justice 322.

2.8.6 Tools/mechanisms addressing the need for confidentiality

Victims of IBSA often experience exacerbated harms due to the 'unwanted subjection to public scrutiny'[540] when seeking redress. Traditional avenues of redress as provided by the systems of criminal justice and civil law generally require the public identification of victims which can result in re-traumatisation. Often the details of court cases will be reported in the press.

An individual complaints mechanism allows victims to report their image without a public record being made. Victims can report their image to the IBA portal without fear of public record or police questioning.

2.9 Conclusion

This chapter identified that the increased criminalisation of IBSA in Australia has not been a panacea for the challenge of IBSA. Issues around anonymity, jurisdictional challenges, and issues with law enforcement resources and training have all hindered the effective combating of IBSA and highlighted the need for a supplementary response. In particular, a need for a specialist body, with expertise in internet regulation and a mandate in the area of IBSA was identified. A key response of the Australian system to the challenge of IBSA was the development of the OESC IBA portal which provides a complaints mechanism for victims of IBSA.

This chapter also examined the development of the OESC from an idea, to its early years as the Office of the Children's eSafety Commissioner, to its expanded powers and responsibilities under the Enhancing Online Safety Act 2015 through to its current state under the Online Safety Act 2021. Understanding how the OESC evolved over time, particularly in relation to the legislation prior to the establishment of the Online Safety Act 2021 provides a deeper understanding of its expanded powers and also provides insight into how Ireland may establish a similar Office. In particular, it was found that the scope of protection provided by a regulatory body should not be age restrictive. The OESC started as a body designed to protect children but then needed to expand to cover all Australians. As is often the case in internet regulation, initial discussions in Australia

[540] Mary Anne Franks, 'Unwilling Avatars: Idealism and Discrimination in Cyberspace' (2011) Columbia Journal of Gender and Law.

about such a body were only focused on protecting children online however once the regulatory body was established it was soon discovered that such a body would need to expand its remit. The incremental growth in OESC powers and scope meant that the OESC developed competence and expertise over time.

This chapter also conducted a desk-based assessment of the functions of the OESC in the context of IBSA which were in place prior to the passing of the Online Safety Act 2021. This was conducted through an examination of the OESC annual reports, the Briggs report, and submissions made to the Government regarding the review of the Enhancing Online Safety Act 2015. While the desk-based assessment provided valuable insight into the practical functioning of the reporting mechanisms of the OESC, the assessment also identified important questions which need to be addressed in order to assess the overall impact and role of the OESC in combating IBSA in Australia.

The Cyberbullying Complaints Scheme was the first reporting mechanism of the OESC and therefore was the first mechanism to be discussed. The key findings from the desk-based research found that while the annual reports from 2015 to 2018 include information on the time frames from when a complaint is received to when it has been investigated and deemed to be cyberbullying material, the annual reports from 2018 to 2021 do not include information on these time frames. This is valuable data which should be recorded and made publicly available as it provides insight into how quickly a report is responded to. Prompt response and investigation is vital to ensure that the OESC can take action through the issuing of a removal notice or remedial direction in a timely manner. The publication of this information would provide a clear indication of whether the scheme is operating in an effective manner and could also be used to identify negative trends that may require corrective action. While the Online Safety Act 2021 requires specific information to be reported in the annual reports, it does not require information on investigation time frames. It is also unreported as to whether cyberbullying material reported to the OESC remains offline permanently (or even for an extended period) or whether victims experience revictimization through the material resurfacing on other platforms by either the original or new perpetrators. Understanding whether reported material remains offline once reported to the OESC would provide a better understanding as to whether victims of IBSA would be able to regain control of their intimate images. While this is likely to be a challenging task, indeed an impossible task to achieve in every instance, a system for recording repeated infractions is necessary to provide insight into the true effectiveness of the system and to help identify where additional action may be needed. The annual reports show that the OESC has not yet had to use its statutory powers

under the Cyberbullying Complaints Scheme. One reason given for this is due to the collaborative work by the OESC with social media platforms through the two-tiered scheme. As a result, the statutory powers of the IBA portal may be deemed excessive. However, the threat of a penalty increases cooperation therefore showing the necessity of these powers.

The key findings from the desk-based assessment of the Online Content Scheme found that the use of a more general scheme which targets harmful content is less likely to be effective in the targeting of IBSA as, depending on its drafting, it may fail to capture many instances of IBSA. This was the case in the context of the Online Content Scheme where the definition of 'class 1' and 'class 2' material referring to 'matters of sex', 'explicitly depict sexual or sexually related activity' and 'explicitly depict nudity or describe or impliedly depict sexual or sexually related activity' would not include all instances of IBSA. This reflects the benefits of introducing specific legislation to ensure that identified harms are fully addressed and once specific legislation is designed, the importance of developing comprehensive definitions to ensure that gaps in protection do not exist.

While the OESC can request a provider located overseas to remove harmful content, the OESC has no power to enforce such as request. In the context of CSAM reported through the Online Content Scheme, where content was hosted overseas and the OESC was unsuccessful in assisting in the removal of such content, it reported the CSAM to INHOPE. An international established network to remove targeted content is very useful. Consideration must be afforded to the adoption of a similar approach in the context of IBSA.

The key findings from the desk-based assessment of the IBA reporting mechanism identified this tool as valuable. Since the implementation of this reporting tool in 2018 to 2021, there has been an increase in the number of reports received. Based on review of available publications, the IBA portal appears to provide a clear, quick, cost effective, and safe mode of complaint and means of redress supplementary to the pursuit of criminal prosecution or civil claims. Similar to the Cyberbullying Complaints Scheme, there is a lack of information published about the success of the OESC in assisting in the removal of intimate images permanently – or for an extended period – and it does not appear that the OESC has a system for recording and reporting reoccurring abuse. As a result, such a reporting system is necessary to identify the true effectiveness of the IBA reporting mechanism and to also help identify where additional action may be needed by the OESC. From 2018-2021, the recipient of a removal notice, from the OESC, had to remove the

identified intimate image within 48 hours. While 48 hours might not seem to be overly long in the abstract, in the internet context, where images have the potential to be distributed instantaneously to a global audience, the need for a rapid response is vital. It is a positive development that the Online Safety Act 2021 reduced the timeframe that online services and end users are granted to respond to an OESC removal notice to 24 hours across all reporting mechanisms. This highlights the importance of efficient processes in the context of the removal of harmful online content and indicates a clear intention on behalf of the Australian legislator to impose robust regulatory obligations on services distributing content online.

This chapter offered an outline and analysis of the Australian response to IBSA examining the legislative response through criminal laws at state/territory and federal level, and the development of a regulatory system and supporting statutory authority with powers to tackle IBSA. In conducting this analysis particular reference was made to victim's needs and how the system addressed and responded to such needs of IBSA victims. Building upon this analysis, drawing from influential research in the field of IBSA and from the chapter's desk-based assessment of the Australian situation, this chapter identified and outlined six key needs of IBSA victims and identified and outlined eight tools/mechanisms that can be used to address the harms caused to victims informing a victim-centred approach to IBSA which is further refined in later chapters. The table and accompanying discussion in section 2.9 illustrates the relationship between these needs and tools/mechanisms. This table is used in later chapters to assess how the needs of victims are being addressed and what improvements might be possible through change in law and policy.

The key findings identified in this chapter form the basis for the development of interview questions and discussions in Chapter 3. The overview of the Online Safety Act 2021 conducted in this chapter highlights key areas of change in the context of the IBSA and thus further informs discussions in Chapter 3, Chapter 4, and Chapter 5. While the analysis of the powers and operation of the OESC prior to the Online Safety Act 2021 formed the basis for the development of interview questions, the discussion of the Online Safety Act allows the author to examine whether issues raised during the interviews in Chapter 3 have been affected or unaffected by the newly implemented law. Changes made in the Online Safety Act also provide an additional comparator to be considered in the discussion of the Irish regulatory response in Chapter 5.

Chapter 3: Semi-structured interviews with experts: Considering the design, impact, and practical operation of the eSafety Commissioner

3.1 Introduction

While there is academic commentary considering the structure of the Office of the eSafety Commissioner (OESC) and its expanding functions,[1] there is a dearth of research considering the perspectives of stakeholders on the practical operation of the OESC. As discussed in Chapter 2, the OESC publishes much useful information – including its annual reports – on the eSafety Commissioner website, yet there are still many unanswered questions.[2] While the official publications provide insight into the operations of the OESC, an essential goal of this project is to seek out and consider the perspectives of independent experts and stakeholders that engage with the OESC. This chapter addresses a gap in the literature by reporting on the semi-structured interviews conducted by the author with key stakeholders and analyses the key insights obtained.

As noted in Chapter 2, these interviews were conducted when the OESC governing legislation was the Enhancing Online Safety Act 2015. As a result, the insights gained are in relation to the law at the time the interviews were conducted. Valuable insight can be gained from these experiences which can inform the development of a regulatory response to online harm in Ireland. This chapter does not ignore the changes in the law made subsequent to the interviews, however, and an additional layer of analysis is added by considering how the Online Safety Act 2021 affects the insights gained from the interviews. Where the Online Safety Act changes an issue raised during the interviews, this is noted throughout the discussion.

Firstly, this chapter outlines the interview objectives, ethical considerations and the interview process. A discussion of the logistics of the interviews provides the reader with an understanding of the process, leading to greater transparency. Secondly, this chapter discusses the interviews conducted with key stakeholders in Australia. For the purposes

[1]See for example - Majid Yar & Jacqueline Drew, 'Image-Based Abuse, Non-Consensual Pornography, Revenge Porn: A Study of Criminalization and Crime Prevention in Australia and England & Wales' (2019) 13 International Journal of Cyber Criminology 578, 585; The Senate, Legal and Constitutional Affairs References Committee, *Phenomenon colloquially referred to as 'revenge porn'* (February 2016).
[2] Office of the eSafety Commissioner, 'Annual Reports' < https://www.esafety.gov.au/about-us/corporate-documents/annual-reports> accessed 15 December 2020.

of this research project, 'stakeholders' are defined as key actors pertaining to issues of online regulation.[3] In addition, this project aims to draw on the experience of officials working in the OESC. The official publications are a vital resource but interviewing staff members directly was identified as an opportunity to delve further into the operation of the OESC in a targeted manner. The interviews were conducted with the intention of obtaining insights that can inform policy discussions taking place in Ireland. Finally, this chapter applies the victim-centred framework developed in Chapter 2 to assess how well the identified tools/mechanisms specific to the Australian context address the identified victim needs using insights gained from the interviews. Consequently, the table from Chapter 2[4] is reintroduced and reconsidered in light of insights gained from the conducted interviews.

A clear and diversely informed understanding of the operation and impact of the OESC and its potential to address the needs of victims is essential in order to adequately assess the merit of the system provided for in Ireland under the recently enacted Online Safety and Media Regulation Act. Policy recommendations made in this thesis aim to build on the successes and avoid any failures identified in the Australian system.

3.2 Justification

The semi-structured interviews conducted received ethical approval in line with the requirements mandated by the Social Research Ethics Subcommittee at Maynooth University. The semi-structured interviews were carried out with non-vulnerable professionals in order to develop a deeper and more diverse understanding of the OESC. Interviews were conducted on the basis of Bogner and Menz's model of expertise, which encompasses technical, process and interpretative knowledge.[5] This particular model believes that interviewing experts is not only a more efficient method of data collection, but also of obtaining extremely succinct and reliable information.[6] Although the subjects

[3] See Appendix for interview information sheet and consent form.
[4] See section 2.9.
[5] Alexander Bogner & Wolfgang Menz, 'The Theory-Generating Expert Interview: Epistemological Interest, Forms of 39 Knowledge, Interaction' in A. Bogner & ors (eds.), *Interviewing Experts* (Palgrave and MacMillan, 2009) 52; Michael Meuser & Ulrike Nagel, 'The Expert Interview and Changes in Knowledge Production' in A. Bogner & ors (eds.) *Interviewing Experts* (Palgrave and MacMillan, 2009) 24.
[6] Alexander Bogner & Wolfgang Menz, 'The Theory-Generating Expert Interview: Epistemological Interest, Forms of 39 Knowledge, Interaction' in A. Bogner & ors (eds.), *Interviewing Experts* (Palgrave and MacMillan, 2009) 52; Michael Meuser & Ulrike Nagel, 'The Expert Interview and Changes in Knowledge Production' in A. Bogner & ors (eds.) *Interviewing Experts* (Palgrave and MacMillan, 2009) 24.

were chosen based on their different kinds of expertise, '[i]t is not the experts themselves who are the objects of the investigation; their function is rather that of informants who provide information about the real objects being investigated.'[7] Semi-structured interviews were conducted with NGOs, charitable organisations, legal practitioners, academics/experts, governmental organisations and departments, advocacy groups, internet freedom organisations, online intermediaries and technology industry bodies. Semi-structured interviews were deemed appropriate because they enabled the design of predetermined questions and allowed for divergence and opportunities to probe beyond the original questions for additional detail. As Muncey described, qualitative data is needed to help explore and discover the perceptions and subjective perspectives of participants about the complexity of their world.[8] The different perspectives provided by each group of expert interviewees not only furnishes the thesis with a better contextual understanding of how the OESC operates in practice, but also provides insight into how the body is viewed internally by members of the OESC team as well as by other concerned parties.

3.3 Preceding the interview

3.3.1 Ethical consideration and approval

'Ethics' are concerned with the right and wrong of a decision or action. There are several reasons why it is important to adhere to ethical norms in research. Ethics promotes the aims of research, such as knowledge, truth, and avoidance of error; ethical standards promote the values that are essential to collaborative work, such as trust, accountability, mutual respect, and fairness; and ethical norms help to ensure that researchers can be held accountable to the public.[9] Furthermore, ethics ensures the quality and integrity of research and promotes social responsibility, human rights, compliance with the law, and health and safety.[10] For the purposes of this study, the author made an application for

[7] Alexander Bogner & Wolfgang Menz, 'The Theory-Generating Expert Interview: Epistemological Interest, Forms of 41 Knowledge, Interaction' in A. Bogner & ors (eds.) *Interviewing Experts* (Palgrave and MacMillan, 2009) 47.
[8] Tessa Muncey, 'Does Mixed methods constitute a change in paradigm? In: Andrews, S; Halcomb, E eds. *Mixed Methods Research for Nursing and the Health Sciences*, 2009 (Chichester: Wiley Blackwell).
[9] David Resnik, 'What is Ethics in Research & Why is it Important?' (2011) National Institute of Environmental Health Studies.
[10] ibid.

ethical approval to the Social Research Ethics Subcommittee at Maynooth University under tier 2 (criteria 1).[11] This research fell within tier 2 (criteria 1) as:

1. The research involved the interviewing of NGOs, charitable organisations, legal practitioners, academics, governmental organisations and departments, advocacy groups, internet freedom organisations, online intermediaries and technology industry bodies, on the functioning of the eSafety Commissioner in practice when removing intimate images online.
2. Interviews were conducted with non-vulnerable adults with explicit consent.
3. Interviewees were broadly identified through their organisation or occupation unless agreement to direct identification was given. If no identification was permitted, pseudonyms were utilised.
4. The interviews were focused on the functioning of the eSafety Commissioner processes, therefore the material is of a non-sensitive nature.
5. No victims of IBSA were interviewed.

Permission was granted in November 2018. A copy of the ethical approval letter is included in the appendices.

Overall interview objectives

These interview objectives, set out below, consider both the overall research aims and ethical standards:

- To gain an insight into the functioning of the OESC.
- To establish whether the OESC is perceived as playing an effective role in addressing the harms of IBSA.
- To gain insight into the logistics of removing intimate images, including on matters such as time frames for removal.
- To establish the merits and limitations of the OESC as perceived by the stakeholders.
- To understand how the OESC body is viewed by the interviewees.
- To gain expert insight into OESC practices related to freedom of information, due process and intermediary responsibility.

[11] Criteria 1 - Research involving adults (with the exception of those identified *vulnerable*) where the material is of a non sensitive nature where the research subjects may be identified either directly or through a key/indicators linked to subjects. This includes surveys, interviews and/or observational studies.

3.3.2 Sampling and selection of Interviewees

One of the crucial tasks in designing a research study is deciding the number and characteristics of the participants invited to participate. In this study, purposive sampling was identified as the most appropriate technique. Purposive sampling is the 'deliberate choice of a participant due to the qualities the participant possesses'. [12] It assumes that a researcher's knowledge about the population can be used to hand pick the participants to be included in the sample. The researcher decides what needs to be known and sets out to find people who can and are willing to provide the information by virtue of knowledge or experience.[13] Purposive sampling is used in the collection of descriptive data and is seen as a useful method to explore participants' perceptions and subjective views.[14] Unlike random studies, which deliberately include diverse participants, purposive sampling concentrates on people with particular characteristics who will better be able to assist with the relevant research.[15] Purposive sampling was used to select individuals and organisations who have publicly engaged with the OESC or who are engaged or professionally interested in the subject matter of IBSA or online harmful content. The purposive sampling allowed for the selection of 67 potential participants from a broad range of backgrounds who engage with the topic of online regulation and/or IBSA specifically. The population comprised key stakeholders of online regulation as represented in the table below.

[12] Ilker Etikan, 'Comparison of Convivence Sampling and Purposive Sampling' (2016) 5(1) American Journal of Theoretical and Applied Statistics.
[13] H Russell Bernard, *Research Methods in Anthropology: Qualitative and Quantitative Approaches* (3rd edn, Alta Mira Press 2002).
[14] John W. Cresswell, & Vicki L. Plano Clark, *Designing and Conducting Mixed Method Research* (2nd edn, Sage 2011).
[15] Michael Q. Patton, *Qualitative research and evaluation methods* (3rd edn, Sage, 2002).

Stakeholder	Number of participants
Non-Governmental Organisations/ Charitable Organisations	17
Legal Practitioners	5
Academics/Experts	20
Governmental Funded Organisations/ Governmental Departments	13
Advocacy Groups	3
Internet Freedom Organisations	1
Online Intermediaries	5
Technology Industry Bodies	3
Total	**67**

Figure 7 Table representing the total number of sent invitations

Access to the participant sample was gained through direct contact with the participants or through contact with their organisation. A formal invitation via e-mail requesting participation was sent to the relevant people. Upon acceptance of the invitation, a follow up e-mail was sent to arrange a place or medium for the meeting and also a date and time. An information sheet and consent form were also attached at this stage. These documents are included in the appendices. Participants were given the option to be interviewed in person in Melbourne, within the participant's primary place of employment, or at an alternative location upon request by the participant, or virtually via Skype. Due to the financial and temporal limitations, it was deemed unfeasible to travel throughout Australia in order to interview each participant in their locality. Accordingly, Melbourne was chosen as the location for face-to-face interviews. Melbourne was chosen as the base for the interviews for a variety of reasons. It is home to one of the Offices of the OESC,

the majority of the identified sample were located in Melbourne, and the researcher identified a relevant conference being held at the University of Melbourne which allowed for knowledge exchange, research dissemination and further participant sampling. Once a format (in-person or virtual), time and place were agreed, a confirmation telephone call (if a contact number was given) or another email was made/sent a few days prior to the interview to remind individuals of the interview. Out of the sample of 67 potential participants, 36 responses were received. 19 of these responses agreed to an interview while 11 declined. Regrettably, the 19 positive responses were not reflective of the interviews actually conducted. Some later declined an interview, some made no further contact after agreeing, and some cancelled due to unforeseen circumstances and were unavailable to arrange an alternative date. The main reasons given for declining an interview were busy schedules, the potential interviewee's belief that they would not be able to contribute to the research, or the potential interviewee's belief that their (or their organisation's) written submission to the statutory review process of the OESC encompassed everything they wished to say about the topic.[16] Six responses indicated that an interview was not suitable and would prefer a written-based interview so that they could review the questions without having to answer in real time. In these cases, a questionnaire was circulated which largely mirrored the questions which would have been asked in a face-to-face interview. Out of the six requested text-based interviews, five of the participants were internet intermediaries while one was a government funded organisation. No responses were received from these questionnaires. Out of the 67 participants invited to an interview, 31 provided no response. As a result, 12 interviews were conducted with 14 participants.

3.3.3 Informed Consent/Confidentiality

Informed consent governs and regulates participation in research.[17] It implies that the researcher has made the most honest effort possible to ensure that the participants understand the risks and benefits of participating in the study, they are informed about their rights not to participate and are presented with information that is free from overt or

[16] Access to the submissions can be found at: Australian Government, 'Reviews of the Enhancing Online Safety Act 2015 and the Online Content Scheme' < https://www.infrastructure.gov.au/have-your-say/reviews-enhancing-online-safety-act-2015-and-online-content-scheme > accessed 20 February 2022. Analysis of these submissions are integrated into Chapter 2 discussions.
[17] Gerard Tobin & Cecily Begley, 'Methodological Rigour within Qualitative Framework' (2004) 48(4) Journal of Advanced Nursing 388.

covert coercion.[18] In this study, all interviewees received an information sheet and consent form prior to the interview. On the day of the interview, the information sheet was explained, and the interviewee was given time to ask any questions before commencing the interview. The researcher ensured the consent form was signed prior to commencement of the interview. Interviewees were also informed that they could withdraw their consent at any stage during the interview or after but that they must do so before the submission of the research.

Confidentiality and anonymity are important considerations in ethical research. Confidentiality involves 'the disclosure of personal information and entails the right to privacy; anonymity involves the disclosure of a person's identity and entails the right to remain unidentified'.[19] Both concepts are inextricably connected; confidentiality can often be accomplished by the use of anonymity. In this research project, interviewees had the option to be identified by an allocated pseudonym, partially identified (i.e. through their organisation or their role within their organisation but not their own name), or fully identified by their name (and organisation, where applicable). The options of full or partial identification were offered as none of the participants were victims of IBSA but rather all non-vulnerable professionals and several participants were already participating publicly in the debate. In spite of this, it was recognised that some participants – such as legal practitioners or governmental organisations – may not wish to make their position public. Accordingly, the researcher anonymised any data collected from these interviews upon request and ensured the anonymity of the participant and organisation. The consent form also afforded interviewees control over how their data would be used in the research. The interviewee could agree or not agree to the use of quotations or extracts from their interview. Confidentiality and anonymity are also vital concepts post-interview and therefore will be discussed in section 3.4.

3.3.4 Key themes of the interview questions

[18] Kader Parahoo, *Nursing Research: Principles, Process and Issues* (2nd edn, Basingstoke: Palgrave 2006) 7.

[19] Benjamen Baez, 'Confidentiality in Qualitative Research: Reflections on Secrets, Power and Agency' (2002) 1(2) Qualitative Research 35.

Pre-determined questions were identified prior to interview. These questions were broken down into specific themes. However, where these were unsuitable to the interviewee, the question was not asked or was altered to suit.[20] The key themes were:

(1) **Engagement:** Under this heading, the interviewee was asked to explain their involvement with the OESC. This included collaborative projects, submissions to the OESC, or any referrals to the OESC.

Sample question

- Have you had any engagement with the eSafety Commissioner/OESC? If so, what sort?

(2) **Process of removing harmful content through the OESC mechanisms:** Here, the questions focused on how the systems of removal operate in a more specific sense. This included but was not limited to the IBA portal. The Cyberbullying Complaints Scheme and the Online Content Scheme were included as they have been in operation for longer than the IBA portal. This allowed interviewees who actually engaged with processes of removal to give an account of what happened during the process. Also, these questions allowed all participants to give their personal understanding of how these systems work and their opinion on these processes.

Sample questions

- Have you engaged with the IBSA portal, Cyberbullying Complaints Scheme, Online Content Scheme? If so, what was the nature of the content?
- Can you describe the process of requesting the removal of harmful content such as intimate images through the OESC?
- Does the OESC remove harmful online content such as intimate images in an effective manner?
- In your opinion does this process provide an effective remedy for victims of IBSA?

[20] Michael Meuser & Ulrike Nagel, 'The Expert Interview and Changes in Knowledge Production' in A. Bogner & ors (eds.) *Interviewing Experts* (Palgrave and MacMillan, 2009) 31.

(3) **Considering the appropriateness of the OESC expanded powers:** Questions under this heading focused on whether the OESC is equipped to establish whether content is harmful and should be removed upon request. Questions under this heading also allowed interviewees to comment on the eSafety Commissioner's expanded powers under the civil penalty regime which was in place at the time under the Enhancing Online Safety Act 2015. Furthermore, these questions enabled discussion on issues of free speech and due process.

Sample questions

- Is the eSafety Commissioner's legislative power of imposing fines for non-compliance under the civil penalty regime effective?
- Is the OESC equipped to establish whether an image is of an intimate nature and should be removed?
- Does the process of removing harmful content by the OESC pose issues for freedom of expression and due process?

(4) **The intermediary debate:** This theme allowed interviewees to give their opinion on the question of intermediary liability and comment on the topic of self-regulation as an alternative.

Sample question

- Is self-regulation of intermediaries via internal company policies or industry-agreed codes of practice a viable solution or is a governmental response – such as the system operated through the OESC – necessary?
- Are intermediaries equipped to establish whether material is considered harmful and should be removed from their platform?

- Should online services be liable for third-party content hosted on their platform?

(5) **Improvements:** Here, interviewees were given the opportunity to provide their opinion on any issues that they have identified with the operation of the Australian system (particularly with regard to the operation and powers of the OESC), to make suggestions on how the system could improve, and/or comment on any successful aspects of the system.

Sample question

- If you could change anything about the OESC, what would it be?

3.3.5 Specific stakeholder category goals

Prior to interviews, the researcher established the importance of each stakeholder category and identified the key data to be found during the interviews.

NGOS/ Charities – The objective for meeting with this sector of stakeholders is to dissect the participants' engagement with the OESC on behalf of IBSA victims who seek/sought their help. The aim of these interviews is to unearth whether these organisations believe the functioning of this body is useful to victims of IBSA in practice. These interviews also aim to establish whether the OESC collaborates with NGOs and charities, and whether the presence or not of collaboration facilitates the eSafety Commissioner's overall functions.

Legal Practitioners – The focus of meeting with this category is to dissect the participants' engagement with the OESC. Interviews focus on whether the body is recommended or are there alternative legal routes available to victims which legal practitioners believe better remedy victims.

Relevant Government Departments and Government Funded Organisations – The aim for meeting with the OESC and related bodies is to delve into questions not addressed in the annual reports. These interviews also aim to establish the level of engagement the OESC has with online intermediaries.

Academics– The focus for meeting with academics is to ask them for their opinion on the powers of the OESC. Specifically, participants are asked to comment on how the OESC fits in the greater debate on intermediary liability. Overall, the questions aim to determine whether the academics interviewed believe that the OESC and surrounding system provide an effective response to IBSA.

Online Intermediaries – These interviews aim to provide insight into the relationship between online intermediaries and the OESC. Participants are asked how many removal requests have been made by the OESC to the company. Also, participants are asked to comment on whether fines have been imposed on the company or whether legal action has been taken against the company by the eSafety Commissioner.

Internet Freedom Organisations and Technology Industry Bodies – The aim of these interviews is to focus on the effect of the OESC on industry.

3.4 The Interviews

Semi-structured interviews were conducted with non-vulnerable professionals during the months of July 2019 and August 2019 in Melbourne, Australia. In total, 12 stakeholder interviews with 14 participants were conducted. There were, in total, ten female and four male participants. Ten interviews were conducted in-person at the participant's workplace or at an alternative location chosen by the participant. Two of the interviews were conducted virtually via Skype as the participants were not located in Melbourne. Three participants from the OESC were interviewed together. Three participants from the Alannah and Madeline Foundation were interviewed separately.[21] The table below represents the number of interviews conducted within each stakeholder category.

Stakeholder	Number of interviews
Non-Governmental Organisations/ Charitable Organisations	4
Legal Practitioners	2
Academics/Experts	3
Government Funded Organisations/ Government Departments	2
Technology Industry Bodies	1
Total	**12**

Figure 8 Table representing the number of interviews conducted per stakeholder category

Each interview lasted no longer than 60 minutes with a ten-minute briefing on the research project and an opportunity for any concerns or questions prior to the interview. Each interviewee was given a consent form to read and sign. Where the interview was conducted via Skype, the interviewee was asked to read and sign the consent form in advance and to scan and email the consent form prior to the interview date. All interviews

[21] These include 'Alannah and Madeline Foundation representative 1', 'Alannah and Madeline Foundation representative 2' & 'Alannah and Madeline Foundation representative 3'.

were voice recorded. During the interviews, all interviewees were asked pre-determined questions as per the established themes. The researcher actively listened to all responses. If the participant's response was inaudible or unclear the researcher asked the participant to repeat their response. Alternatively, the researcher would repeat what was heard and would ask for clarity. It was important that the researcher did not influence responses and therefore clarity was only requested using the same phrases/word/term as the participant. The progression of each interview was highly dependent on the nature of the experiences and responses of each participant. The semi-structured interview process facilitated greater focused discussion where the opportunity arose. When closing the interview, the researcher thanked the participant for their contribution and confirmed that the transcript of the interview would be sent to them for review.

3.5 Post-Interview

After each interview the researcher engaged in social conversation with the participant. Each participant was given a business card with contact details of the researcher and were advised to make contact if they wished to discuss any aspect of the interview process.

3.5.1 Transcription

Each interview was recorded on an audio recorder, before being transcribed in full. This, as well as the other parameters of the interviews and the research project as a whole, was made known to the participants in the invitation letter and in the information and consent forms that were given to them before the interview commenced. Each interview was transcribed verbatim by the researcher following each interview and before conducting subsequent interviews where possible. Transcripts were sent to each interviewee for review.

3.5.2 Confidentiality/data storage

Only the researcher and supervisor of the project saw the original transcripts as set out in the information sheet provided to interviewees. Once the transcription was completed, the recordings were deleted, and the transcripts were encrypted and kept password protected on the researcher's laptop which was kept in a secured cabinet in the researcher's office.

As per the information sheet provided to interviewees, participants had three options for identification. They could agree to full identification whereby they would be identified by name and their organisation's name where appropriate. Participants could agree to partial identification whereby they would be identified by their organisation's name and not their own name, or their own name but not attached to their organisation. Finally, participants could choose full anonymity whereby their identity would be fully concealed. If an interviewee chose to be anonymised, their identity was protected by referring to them by a pseudonym. The identification key of pseudonyms was encrypted and kept password protected on the researcher's laptop. Out of the 12 interviews with 14 participants, six agreed to full identification, seven agreed to partial identification (with six choosing to be identified by their organisation's name and one choosing to be identified by their own name), and one participant agreed to full anonymity. One participant who agreed to some level of identification, requested that certain parts of the transcript remain anonymous. This is represented in the table below.

The researcher and supervisor alone have access to the file of names and pseudonyms. After a period of ten years following completion of the project, all transcripts and electronic files (together with the code to pseudonyms held by the researcher and supervisor) will be deleted. Any paper record referencing the interview data will be shredded. This was outlined in the information sheet provided to participants.

Participants were notified via the information sheet that the results of the qualitative study will be seen by the researcher, supervisor and examiners, and will be presented in the published thesis, academic publications, and conferences.

Stakeholder Category	Identification
Non-Governmental Organisations/ Charitable Organisations	3 Representatives from The National Centre Against Bullying (NCAB), an initiative of the Alannah & Madeline Foundation
Non-Governmental Organisations/ Charitable Organisations	Helen Campbell OAM Executive Officer Women's Legal Service NSW
Legal Practitioners	Peter Clarke (Barrister)
Legal Practitioners	EJ Wise from Wise Law[22] (Solicitor and cybersecurity expert)
Academics	Dr Bianca Fileborn (Opted not to be associated with institution)
Academics	Dr Nicola Henry RMIT University
Academics	Dr Nicolas Suzor Queensland University of Technology
Government Funded Organisations/ Government Departments	Anonymous
Governmental Funded Organisations/ Governmental Departments	3 Representatives from the OESC
Technology Industry Bodies	Christiane Gillespie-Jones from Communications Alliance
Total	**12 interviews** **14 participants**

Figure 9 Table identifying interviewees

[22] Wise Law <https://wiselaw.com.au/> accessed 24 February 2022.

Interviewees	Thesis Identification Key
3 Representatives from The National Centre Against Bullying (NCAB), an initiative of the Alannah & Madeline Foundation	• 'Alannah & Madeline Foundation representative 1' • 'Alannah & Madeline Foundation representative 2' • 'Alannah & Madeline Foundation representative 3'
Helen Campbell OAM Executive Officer Women's Legal Service NSW	Helen Campbell
Peter Clarke (Barrister)	Peter Clarke
EJ Wise, Wise Law (Solicitor and cybersecurity expert)	EJ Wise
Dr Bianca Fileborn (Opted not to be associated with institution)	Bianca Fileborn
Dr Nicola Henry RMIT University	Nicola Henry
Dr Nicolas Suzor Queensland University of Technology	Nicolas Suzor
Anonymous interviewee from the stakeholder category of Government Funded Organisations/Government Departments	'Anonymous interviewee 1'
3 Representatives from the OESC	• 'OESC representative 1' • 'OESC representative 2' • 'OESC representative 3'
Christiane Gillespie-Jones Communications Alliance	Christiane Gillespie-Jones
Identified interviewee who requested anonymity for certain parts of interview	'Anonymous interviewee 2'

Figure 10 Thesis identification key

3.5.3 Analysis Process

In this study, a thematic analysis was conducted. Boyatzis describes thematic analysis as a process for encoding qualitative information.[23] He explains that the encoding requires an explicit 'code'.[24] He further describes how this code may take many forms and includes a list of themes which may be generated from the qualitative data or generated deductively from prior research.[25] The thematic analysis employed in this study is facilitated using framework analysis consisting of five key stages as adopted from Richie, Spencer, and

[23] Richard Boyatzis, *Transforming Qualitative Information: Thematic Analysis and Code Development* (Sage, 1998).
[24] ibid.
[25] ibid.

O'Connor, and Srivastava and Thomson including: data familiarisation, identifying a thematic framework, indexing, charting, and mapping and interpretation.[26]

Familiarisation Phase

Familiarisation refers to the process during which the researcher becomes familiarised with the transcripts of the data collected.[27] Consequently, the researcher read all the transcripts and relistened to the audiotapes. According to Boyatzis, the process of paraphrasing and summarising interview data allows for information to enter into the researcher's 'unconscious' as well as allowing for the 'conscious processing' of information.[28] As a result, the interviewer became increasingly familiar with the interview data through re-reading, re-listening and summarising the raw data. During this process, the researcher became immersed in the data and started to become aware of key ideas and recurrent themes. The researcher noted these. Broad sections within the transcripts which fitted into the themes were identified.

Identifying a thematic framework

Identifying a thematic framework involves the recognition of 'emerging themes or issues in the data set'.[29] These emerging themes or issues may have arisen from pre-established themes identified prior to the interviews or they may be established after the familiarisation phase.[30] In this project the researcher identified five themes prior to conducting interviews:

1. Engagement
2. Process of removing harmful content through the OESC removal mechanisms
3. Considering the appropriateness of the OESC expanded powers
4. The intermediary debate
5. Improvements

[26] Jane Richie, Liz Spencer & William O'Connor, 'Carrying Out Qualitative Analysis' in Jane Ritchie and Jane Lewis (eds) *Qualitative Research Practice: A Guide for Social Science Students and Researchers* (London: Sage 2003) 219; Aashish Srivastava & S. Bruce Thomson, 'Framework Analysis: A Qualitative Methodology for Applied Policy Research' (2009) 4(2) JOAAG 72.
[27] Jane Ritchie, & Liz Spencer, 'Qualitative Data Analysis for Applied Policy Research' in A. Bryman and R. G. Burgess (eds) *Analyzing Qualitative Data* (Routledge London, 1994).
[28] Richard Boyatzis, Transforming Qualitative Information: Thematic Analysis and Code Development (Sage: USA, 1998) 45.
[29] Aashish Srivastava & S. Bruce Thomson, 'Framework Analysis: A Qualitative Methodology for Applied Policy Research' (2009) 4(2) Journal of Administration and Governance 72.
[30] ibid.

These key themes form the basis of the thematic framework and are used to filter and classify the data.[31] Although the researcher identified priority themes, it was important to maintain an open mind as Ritchie and Spencer stress that the thematic framework is only 'tentative' and there are further chances of refining it at subsequent stages of analysis.[32] This process of devising and refining a thematic framework allows the researcher to ensure that the research questions are being addressed.[33]

Indexing

Indexing involves the identification of portions or sections of the data that correspond to a particular theme.[34] This process was applied to all transcripts of interviews. Ritchie and Spencer recommend that a numerical system be used for the indexing references and to accompany this with annotations in the margin beside the text.[35] The researcher used a colour code to highlight text instead of numbers. Each theme was assigned a colour. Sections of the transcripts which related to the various themes were highlighted using the assigned colour. Analytic memos were inserted beside relevant sections of the transcript to link certain pieces of data with the themes and other concepts linked to literature.

Charting

Charting involves the arrangement of specific pieces of indexed data into charts of the themes.[36] This means that the data is lifted from its 'original textual context' (the transcript) and placed in charts that consist of the headings and subheadings that were 'drawn during the thematic framework, or from a priori research inquiries or in the manner that is perceived to be the best way to report the research'.[37] In this project, the researcher copied and pasted indexed data from the transcript to a separate word-processing document which was categorised into the thematic framework. Great care was taken during this process as Ritchie and Spencer noted that the origin of the data must be

[31] Jane Ritchie, & Liz Spencer, 'Qualitative Data Analysis for Applied Policy Research' in A. Bryman and R. G. Burgess (eds) *Analyzing Qualitative Data* (Routledge London, 1994).
[32] Jane Richie, Liz Spencer & William O'Connor, 'Carrying Out Qualitative Analysis' in Jane Ritchie and Jane Lewis (eds) *Qualitative Research Practice: A Guide for Social Science Students and Researchers* (London: Sage 2003).
[33] Aashish Srivastava & S. Bruce Thomson, 'Framework Analysis: A Qualitative Methodology for Applied Policy Research' (2009) 4(2) JOAAG 72.
[34] ibid.
[35]Jane Ritchie and Liz Spencer, 'Qualitative Data Analysis for Applied Policy Research' in A. Bryman and R. G. Burgess (eds) *Analyzing Qualitative Data* (Routledge London, 1994).
[36]Aashish Srivastava & S. Bruce Thomson, 'Framework Analysis: A Qualitative Methodology for Applied Policy Research' (2009) 4(2) JOAAG 72.
[37] Jane Ritchie, & Liz Spencer, 'Qualitative Data Analysis for Applied Policy Research' in A. Bryman and R. G. Burgess (eds) *Analyzing Qualitative Data* (Routledge London, 1994).

clearly identifiable. As a result, the researcher made sure to label each piece of data either with the name of the interviewee (where identification was agreed) or a pseudonym (where the interviewee wished to remain anonymous).

Mapping and Interpretation

The final stage of analysis involves the mapping and interpretation of the data as laid out in the charts. Data within each code was compared and similar data was identified and re-coded into subcategories. Quotations from the interviews were grouped manually based on the specific themes they addressed as well as whether the interview subjects agreed or disagreed on a given point. These were then interspersed into the analysis that had previously been conducted in order to reflect how each of the interviewees perceived the operation of the OESC based on their specific expertise. Other sources were then inserted alongside these quotations from the interviews where these either agreed or contradicted what had been said by the interview subjects. The researcher then analysed all the organised data and developed an outline for each subcategory's discussion within each theme. The researcher considered the interview objectives when developing these outlines. The researcher ensured that the data gathered from the interviews to develop these outlines 'echoed the true attitudes, beliefs, and values of the participants'.[38] While analysing the interview data, the researcher identified and noted insights that could inform potential recommendations for the Irish context to be discussed in Chapter 5.

3.6 Deriving lessons from the interviews

3.6.1 Theme 1: Engagement

Although the researcher was aware through desk-based research that the interviewees selected for interview are key actors in issues pertaining to online regulation, their actual level of engagement with the OESC was important to establish. This allowed the researcher to identify the level and type of engagement the OESC has with key stakeholders in general but also specifically with the interviewees. Out of the 14 participants interviewed, 11 had direct engagement with the OESC, 2 had indirect engagement with the OESC, and one had no engagement with the OESC.

[38]Jane Richie, Liz Spencer & William O'Connor, 'Carrying Out Qualitative Analysis' in Jane Ritchie and Jane Lewis (eds) *Qualitative Research Practice: A Guide for Social Science Students and Researchers* (London: Sage 2003).

Direct Engagement

11 participants had direct contact with the OESC.[39] This level of engagement ranged from activities such as meeting or talking with OESC staff, working for, with or on behalf of the OESC, promoting the OESC and/or collaborating with the Office.

'Alannah & Madeline Foundation representative 1' and 'Alannah & Madeline Foundation representative 2' explained how the foundation is a trusted eSafety provider and as a result promotes the systems and services operated by the OESC through workshops which have been given to over '50000 people'. Furthermore, both participants explained that the Alannah and Madeline Foundation sit on 'reference groups'/ 'committees' which provide advice and opinions to the OESC.[40] As one interviewee explained:

> So, our experience of the eSafety Commissioner is we are very supportive, and we are on all the committees. We are an accredited provider; we are part of it. ('Alannah & Madeline Foundation representative 1'

The Alannah & Madeline Foundation also directs victims to the OESC and delivers presentations on the OESC. The Alannah & Madeline Foundation representatives stated that they use the OESC resources in carrying out their roles and provide step-by-step information on how to access the eSafety resources and how to find the website.

[39] These included three representatives from the Alannah and Madeline Foundation, three representatives from the OESC, Helen Campbell from Women's Legal Service NSW, Dr Nicola Henry, Dr Nicolas Suzor, Christiane Gillespie-Jones from Communications Alliance and an anonymous Interviewee representing stakeholders from the category of 'Governmental Funded Organisations/Governmental Departments'.

[40] The Alannah and Madeline Foundation clarified via email that there have been various iterations of 'committees/reference groups': 'There was an original advisory committee which had approximately 40 people. This advisory committee also had sub committees for specific issues such as prevention or pornography. This advisory committee has since changed into a smaller committee. It is convened 3 times a year for about 3 hours and includes Government agencies; researchers and representatives of key community groups. It includes approximately 24 members.' See email correspondence with 'Alannah and Madeline Foundation representative 1', on file with author; As set out in the OESC 2020 Annual Report, 'the eSafety Advisory Committee (eAC) is eSafety's advisory forum attended by key representatives from industry, government, civil society organisations and academia. eSafety formed the eAC in early 2020 to replace the Online Safety Consultative Working Group, which did not meet during 2019 while the Statutory Review of the Enhancing Online Safety Act 2015 was conducted. The eAC is tasked with providing technical and policy expertise, research data, coordination and other assistance to eSafety, to ensure Australia's online safety response and support system is consultative, evidence-based, cross-sectoral and effective.' Current members include: eSafety Commissioner (Chair), Alannah and Madeline Foundation, Communications Alliance, Department of Education, Skills and Employment, Department of Home Affairs, Department of Infrastructure, Transport, Regional Development and Communications, Department of Prime Minister and Cabinet, Department of Social Services, Facebook, Google, Macquarie University, RMIT University, Telstra, headspace, Twitter, University of New South Wales, Western Sydney University, and yourtown. See Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2019/20 227.

Similarly, Helen Campbell from Women's Legal Service NSW explained how IBSA is inextricably linked to domestic violence and that text message is the most common form of dissemination reported by their victims. As a result, her organisation directs victims that come to them to the OESC.

Academics, Nicola Henry and Nicolas Suzor had direct engagement by meeting in person and talking with team members of the OESC. Furthermore, Nicola Henry had engaged with the OESC on commissioned projects and presenting at conferences with members of the OESC. She is also a member of the eSafety Advisory Committee[41] and advised on the design and content of the IBA portal.

Christiane Gillespie-Jones from Communications Alliance (which represents technology industry bodies) engaged with the eSafety Commissioner by providing commentary and submissions and worked closely with them during the Christchurch incident.[42]

'Anonymous interviewee 1' from the category of 'Government Funded Organisations/Government Departments' engaged with the OESC through shared responsibilities and both organisations have worked together. The organisation also directs people to the OESC, where appropriate, if they happen to come to their organisation first but where the matter raised would be more suitably addressed by the OESC. The participant revealed:

> We work quite closely with the eSafety Commissioner with regard to overlapping policy responsibilities. ('Anonymous interviewee 1')

[41] Nicola Henry stated she was a member of a consultive group which she described as an advisory group to the eSafety Commissioner which consists of approximately 12 members who are academics or stakeholders and who meet at the Syndney Headquarters of the eSafety Commissioner three to four times a year. See footnote 39 for further discussion.

[42] On the 15th of March 2019, an Australian gunman killed 51 people and injured 50 others in a terrorist attack on two mosques in Christchurch, New Zealand. The gunman live-streamed the first 17 minutes of the attack. The gunman also posted a 'manifesto' online, expressing hate speech and white supremacist rhetoric. The video and manifesto went viral, and rapidly spread across various social media platforms. See Office of the eSafety Commissioner, 'ISP Blocking: facts and falsehoods' (24 March 2020) <https://www.esafety.gov.au/sites/default/files/2020-03/eSafety-ISP-Blocking-factsheet.pdf > accessed 21 July 2020; Dominic Bailey, David Brown, Salim Qurashi, Debie Loizou, Lucy Rodgers & Prina Shah, 'Christchurch shootings: How the attacks unfolded' (BBC, 18 March 2019) < https://www.bbc.com/news/world-asia-47582183 > accessed 24 February 2022; Charlotte Graham-McLay, Austin Ramzy & Daniel Victor, 'Christchurch Mosque Shootings Were Partly Streamed on Facebook' *New York Times* (New York, 14 March 2019).

The researcher also interviewed three representatives from the OESC. These representatives engage with the OESC via policy work, research or as a member of the image-based abuse team.

Indirect Engagement

Out of the 14 interview participants**,** two interviewees indirectly engaged with the OESC. Bianca Fileborn explains how she is aware of the OESC due to her research interests and that she has attended presentations/conferences of the OESC. Peter Clarke has also engaged with the OESC by means of written submission.

No Engagement

EJ Wise had no engagement with the OESC.

Overall, the OESC engages extensively with a variety of stakeholders, including NGOs, legal practitioners, academics, online intermediaries, and technology industry bodies. This was reflected in the interviews where it was found that 13 out of the 14 participants interviewed engaged with the OESC on some level. Furthermore, the OESC fosters engagement through a wide variety of means including reference groups/committees, the trusted eSafety providers scheme, and commissioning research projects. The benefits of such engagement are greater cooperation, more knowledge exchange, increased awareness raising, and an expanded opportunity to connect with victims through referrals. It is important Ireland establishes clear avenues for stakeholders to engage with a similar body in the Irish context.

3.6.2 Theme 2: Process of removing harmful content through the OESC removal mechanisms

The purpose of this theme was to explore the experience and opinions of the stakeholders as regards the IBA portal in place at the time the interviews were conducted. The researcher aimed to understand how the OESC system of removal of intimate images worked, whether the system resulted in intimate images being removed in an effective manner, whether victims are remedied, and whether there is a need for statutory power and the civil penalty regime. Eight sub-themes developed from the information provided during the interviews under this pre-established theme which are: mooted impossibility of the task, rogue websites, the need for statutory power and the civil penalty regime, the importance of a victim's voice, the importance of an alternative route, the symbolic role

of the eSafety Commissioner, and the significance of eSafety Commissioners having a background in the technology industry.[43]

3.6.2.1 Mooted impossibility of the task

Interview responses raised the question of whether the OESC could ever be sufficiently effective in remedying victims of IBSA or helping victims of IBSA. According to Henry, Flynn, and Powell, the main priority of victims is to regain control of the image and later prosecute their perpetrator.[44] Regaining control of an image in the online world may be a task beyond the capabilities of the OESC or any other similar body or organisation. In separate interviews, Bianca Fileborn and the 'Alannah & Madeline Foundation representative 2' both stated that the OESC 'do what they can'. Bianca Fileborn explained that the OESC can only be effective to a certain point and that it is very hard to be sufficiently effective when it comes to removing harmful content online. She noted that it is very hard for anyone, no matter how well-equipped, to remove an image permanently:

> It's incredibly difficult to permanently remove an image … you can take something down but that's not to say it won't pop back up again. It can be incredibly difficult I think to locate every single version of an image that is out there. (Bianca Fileborn)

Similarly, EJ Wise held this view, stating:

> we can't guarantee that the image can either be de-identified or destroyed forever no matter what takedown notice there is. In fact, I think it would be a brave citizen that would put their hand up and say yes I have removed it. (EJ Wise)

Considering the rapid speed at which content spreads on the internet, the OESC may have an impossible task of regaining control of the image on behalf of victims.

---

[43] The first eSafety Commissioner, Alastair McGibbon, spent five years as Head of Trust & Safety at eBay Australia and later at eBay Asia Specific. See The Conversation < https://theconversation.com/profiles/alastair-macgibbon-19023> accessed 15 December 2020. The current eSafety Commissioner, Julie Inman Grant, has extensive experience in the technology sector having worked in safety roles at Microsoft, Twitter, and Adobe. Grant spent 17 years working in Microsoft as the Global Safety Director for safety policy and outreach. At Twitter, Grant headed up Public Policy for Australia and South East Asia, managing a range of public policy issues, including online safety and countering violent extremism. Grant also served as Director of Government Relations Asia Pacific at Adobe, where she worked with governments across the region on issues such as innovation and digital transformation, creativity and STEM. See Human Rights and Technology <https://tech.humanrights.gov.au/julie-inman-grant> accessed 15 December 2020.

[44] Nicola Henry, Asher Flynn & Anastasia Powell, 'Policing Image-Based Sexual Abuse: Stakeholders Perspectives' (2018) 19 Police Practice and Research 565.

According to Henry, Flynn, and Powell the main priority of victims of IBSA is to regain control of the image by having it removed from the internet and devices which store the image.[45] Nicolas Suzor, Peter Clarke and 'Anonymous interviewee 1' confirmed that the OESC is effective in their powers to the extent that they can be. One of the OESC's major barriers when removing harmful online content is the jurisdictional challenges that arise in the regulation of the internet.[46] 'Anonymous interviewee 1' explained that it is hard for the OESC to be effective as some perpetrators may be located outside of Australia, and as a result, the OESC has no power to force these perpetrators to remove an intimate image:

> An organization may be outside of Australia, it can be difficult to enforce, protect our borders and that sort of thing. So it can be you know that the eSafety Commissioner wants to do something, wants to take down a particular piece of footage but simply can't and that may be sort of a function of something bigger than Australia. It could be a function of the way in which the internet works. So that definitely detracts from the effectiveness of her ability to get things done. ('Anonymous interviewee 1')

Peter Clarke stated that while the majority of people use platforms which are based in jurisdictions with an established rule of law 'there are a number of platforms that are based in jurisdictions outside those areas and it's almost impossible to remove those images'.

Nicolas Suzor explains how the OESC is not effective when removing content overseas but that this is due to regulatory restraints that are out of their control:

> There's no real effective way for any Australian regulatory agency to deal with prohibited content that's hosted overseas. (Nicolas Suzor)

'OESC representative 1' acknowledged that in some cases the team struggles to remove the image. However, in such cases the team resorts to their 'failsafe' which is to minimise the visibility of the image online. They do this by requesting to have the image de-indexed from search engines.

> In the very unusual circumstance where we can't get content removed … our failsafe is always we can de-index from Google search results so that way even if we're unable to get the content removed, we know that we minimize the exposure. People can't search for it. ('OESC representative 1')

[45] ibid.
[46] See Chapter 1 section 1.2.4.

Essentially, it is very hard for the OESC to ensure the removal of an intimate image permanently due to the rapid speed at which online content spreads and also the jurisdictional challenges and challenges associated with anonymity. The OESC particularly struggle to bring about the removal of harmful content hosted overseas. The OESC response to these challenges is to request search engines to voluntarily de-index content. The Online Safety Act 2021 empowers the OESC to issue link deletion notices[47] and app removal notices[48] to direct a search engine provider or an app store to remove a link or app which provides access to reported harmful material particularly in cases where the content is hosted overseas, which can ensure the reduced visibility of harmful content. Ireland must consider such alternative actions where the optimum goal of complete removal is not possible.

The OESC is also challenged when trying to carry out its powers to order removal due to the complicated nature of the legal framework. At the time of the interviews the OESC was governed under an array of piecemeal legislation as set out in Chapter 2. In 2021, the Australian Government passed the Online Safety Act 2021 which the Government said would 'consolidate Australia's current legislative framework' (i.e. the legislation in place at the time of the interviews) and 'update it in light of changes to the online environment'.[49] The Briggs report (discussed in Chapter 2) established that there was a need to consolidate the 'disparate elements of legislation' into a single piece of online safety legislation.[50] Under the framework of legislation in place at the time of the interviews there was no clear identified timelines upon which harmful material should be removed. The Online Safety Act includes consistent takedown requirements following a removal notice for the IBA Portal, the Cyberbullying Complaints Scheme, and the Online Content Scheme, requiring all recipients of a removal notice to remove material within 24 hours upon receiving the notice from the OESC.[51]

Another challenge for the OESC to take action was with regard to the classification of content under the Online Content Scheme. Under the legislation in place at the time of the interviews, material reported to the OESC under the Online Content Scheme had to

[47] Online Safety Act 2021, s 124.
[48] ibid s 128.
[49] Australian Government Department of Communications and the Arts, Online Safety Legislative Reform Discussion Paper (December 2019).
[50] Lynelle Briggs, *Report of the Statutory Review of the Enhancing Online Safety Act 2015 and the Review of Schedules 5 and 7 to the Broadcasting Services Act 1992 (Online Content Scheme)* October 2018.
[51] Online Safety Act 2021, s 65, s 77, s 88, s 109, s 114.

be assessed and classified by the Classification Board.[52] This required process caused delays to the OESC's ability to take action as they had to await approval that the content was prohibited. The Online Safety Act 2021 allows the OESC to make an independent assessment of whether the reported material would be classified as 'class 1 material' or 'class 2 material' as per the Classification Code.

Four of the interview participants identified some of these points more generally during the interviews. Christiane Gillespie-Jones, Nicolas Suzor, Peter Clarke, and 'Anonymous Interviewee 1' suggested that the regulatory framework in place at the time of the interviews under the Broadcasting Services Act is ineffective and complicated. Christiane Gillespie-Jones from Communications Alliance confirmed that the OESC cannot rely on the legal framework discussed during the interviews under the Broadcasting Services Act therefore making it impossible to be sufficiently effective when removing online harmful content:

> The eSafety Commissioner is efficient within the legal framework that she has to work with. The legal framework would need revision and is flagged for revision. **(**Christiane Gillespie- Jones)

This viewpoint was also reiterated by another participant:

> Given the limits of what we can actually do in Australian law and the really complicated and quite ineffective existing statutory schemes that we have under the Broadcasting Services Act for the classification of Internet content. So the baseline use of media regulation in Australia just doesn't work at all with Internet content, particularly content hosted overseas. (Nicolas Suzor)

Overall, at the time of the interviews, the OESC struggled to remove content in an effective manner under the Online Content Scheme due to the array of piecemeal legislation contained under Schedules 5 and 7 of the Broadcasting Services Act and the Enhancing Online Safety Act 2015. The Online Safety Act 2021 consolidates the legislation into one Act providing clearer and consistent measures in relation to investigating, issuing notices, and taking enforcement actions for each of the reporting mechanisms provided for under the Act including the Online Content Scheme, the Cyberbullying Complaints Scheme, and the IBA Scheme. Australia has been one of the global leaders in the regulation of online content and its system developed over time and in an incremental manner. Jurisdictions that are more recently seeking to regulate in this

[52] Australian Government Department of Communications and the Arts, Fact Sheet – Online Safety Reform Proposal – Harmful Online Content (11 December 2019).

space tend to adopt a general approach and it is a positive for transparency and legal clarity that a comprehensive approach is now being taken in Australia. Of course, other jurisdictions do not have the benefit of Australia's direct experience over the last number of years in formulating their regulatory approaches, but policy makers in those jurisdictions can at least seek to extract lessons from the study of the Australian system that can be applied in their particular domestic contexts.

3.6.2.2 Rogue websites

Another challenge to the effectiveness of the OESC in removing intimate images is the existence of small platforms or websites which do not wish to collaborate or cooperate with the OESC. Interviews revealed that the OESC has positive relationships with the major social media platforms but struggles to develop such strong relationships with smaller platforms which can affect their overall performance. 'Alannah & Madeline Foundation representative 1' explained that not every platform is equally 'responsible or responsive'. The representative explained that there are a lot of 'cowboy platforms' where nothing happens if you complain about harmful content. Nicola Henry also explained that some of the more 'rogue websites' do not have relationships with Governmental agencies like the OESC making it very difficult for collaboration to happen.

As a result, while the OESC has established strong cooperative relationships with the main online platforms and providers, problems remain with smaller websites that refuse to follow the direction of the OESC. The development of alternative responses is essential where cooperation or legal action fails. While the OESC has responded in such situations by requesting search engines to voluntarily remove access to rogue websites which host such harmful content, the Online Safety Act 2021 empowers the OESC to officially request such removal through a link deletion notice and apply a penalty if the provider fails to comply. Regulatory attempts in Ireland must consider the possibility that action taken against the provider of the harmful content – particularly where the provider is a smaller platform – will not always be successful and as a result an alternative course of action must be established in the legislation so to provide clarity and certainty in how to respond in cases.

3.6.2.3 The need for statutory power and the civil penalty regime

All participants generally endorsed the necessity of the statutory powers of the eSafety Commissioner. However, Nicolas Suzor, Helen Campbell, Peter Clarke, and Christine

Gillespie-Jones raised some issues of concern regarding the lack of use of these powers by the OESC, its lack of effect against rogue websites, and how education may be more effective for prevention and deterrence.

Helen Campbell explained how awareness campaigns are not successful for achieving actual results and therefore the expanded powers (under the Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Act 2018) of the OESC were needed. 'OESC representative 1' highlighted that the mere ability to impose a sanction 'is what spurs people [intermediaries] on to remove content'. Furthermore, Nicola Henry highlighted how the statutory power is essential as without it, the OESC powers have no backbone:

> I think the Australian model is a good one because the statutory legislation behind it does give it weight and I fear that you know an agency that set up that doesn't have any weight that doesn't have any power, that's purely symbolic and kind of plays an indicative function would just lack a back bone. (Nicola Henry)

However, while the need for statutory power was supported, 'OESC representative 1' confirmed that they have not yet had to implement a fine or seek a court order as was also confirmed in the annual reports discussed in Chapter 2. Nicolas Suzor raised doubts about the necessity of statutory power or a civil penalty regime as he stated that while the eSafety Commissioner has statutory power, it does not use it and instead exercises a soft power through fostering relationships with intermediaries. Nicolas Suzor pointed out that they may as well have no statutory power if they are not using it.

> They exercise this sort of soft power to develop relationships with tech companies and get things actioned … they still haven't taken any legal steps to enforce their powers under the act. (Nicolas Suzor)

This view was shared by Peter Clarke who stated that a civil penalty regime is only effective if the Commissioner is willing to implement fines. As no fines have been handed out, he feels that the eSafety Commissioner may be following in the footsteps of the Information Commissioner who has not implemented a fine since 2014.

While Helen Campbell generally supported the need for statutory powers, she also questioned the need for the civil penalty regime specifically in certain contexts explaining that the expanded statutory powers are no more effective than the ability to hand out a notice for removal. She further justified this response by stating that the problem is not big corporations but rather the 'outliers' whose identity is hidden and are hard to locate:

> You still find if you talk to the eSafety commissioner that the problems are the outliers. So the small the unregulated bloke at the back of the shed with a tin can and a piece of string he's not paying any attention to any regulation. And he's probably going to be pretty difficult to find and shut down. (Helen Campbell)

Helen Campbell further explained that the major intermediaries comply with the OESC when requested to remove material and therefore the civil penalty regime is less of a necessity due to the pre-established voluntary compliance levels:

> There is an informal network of regulatory cooperation which is enhancing. So even though you might look at what's on paper or go well there's limits to that regulatory armour and there's been no actual cases taken through it because the high level of voluntary compliance and the non-compliance aren't worth pursuing because they just run away and hide. (Helen Campbell)

Peter Clarke highlights a further limitation of the civil penalty regime by explaining how it is a 'very bureaucratic process' and as a result the process of bringing penalty regime proceedings is 'very slow and for that reason not effective'. He explains that the eSafety Commissioner can impose a fine but a fine can only be enforced if it has an order from the court. However, the court process is slow. Therefore, the image may already go viral by the time an order is sought from the court. Due to this reasoning, Peter Clarke suggests that injunctive relief is a more appropriate approach as the image can be removed immediately and then reposted if no harm is found:

> The more important action that should be taken is some form of injunctive relief. And then you can bring a civil penalty proceeding because injunctive relief is basically saying remove it. Then we'll sort out the nature of the ill or whether it should be returned. Because ultimately the matter is about dealing with the problem immediately because it has an immediate impact on the victim. (Peter Clarke)

Christine Gillespie-Jones explained how her organisation (Communications Alliance) does not normally comment on whether the civil penalty regime is necessary however she explained they were not necessarily against it. However, Christine Gillespie-Jones questioned whether the civil penalty is effective in the bigger picture of prevention of IBSA in the first place and proposed that educative measures may be more appropriate.

> I don't think we were necessarily against it. The biggest problem is. To what extent do you really address the issue just with the civil penalties regime? Don't you have to work additionally far harder on the kids or people not posting the content? And she's [Julie Inman Grant, eSafety Commissioner] doing some work there. And of course, schools are increasingly doing some work in this direction, and it

> would be probably helpful if Australia had a more holistic debate about the Internet content on the Internet…. it would be far better if we or in addition, if we start a debate of educating people in Australia and everywhere to basically use the internet properly. (Christine Gillespie-Jones)

It is important to note that despite some of the limitations of the civil penalty regime as highlighted above, Nicola Henry highlighted that the civil penalty regime is not perfect because it is new. Furthermore, 'OESC representative 1' stated that since the implementation of the civil penalty regime, the removal rate has increased from 80% to 90%:

> It might just be a question of correlation rather than causation but when we started in October 2017 prior to the civil scheme starting, our removal success rate was around 80 per cent. And for the last financial year or since the scheme started, it is at 90 per cent now. So that could be for a range of factors, it could be growing awareness of us and our powers, it could be content providers being a little bit scared of them or it could just be that we're getting better at what we do, and that we're tenacious. ('OESC representative 1')

Overall, there is a need for the statutory powers of the OESC under the IBA scheme however as detailed above, Nicolas Suzor, Peter Clarke, Helen Campbell, and Christine Gillespie-Jones raised concerns. In spite of this, the findings from the interviews indicate strong support for the OESC enforcement powers among the stakeholders interviewed. This supports the development of robust statutory powers for a specialist regulatory body in Ireland. While the OESC process can be assessed as relatively streamlined compared to the criminal justice process, the imposing of an enforcement action including an injunction, enforceable undertaking, or a civil penalty by the OESC requires a court order and this inevitably slows down the process. Nicolas Suzor and Peter Clarke recommended that in order to effectively address the immediacy and scale of distribution in the online sphere, the regulator should be empowered to make a determination and issue an injunction or a civil penalty without a court order, but which can later be appealed to a court.

3.6.2.4 The importance of a victim's voice

'Alannah & Madeline Foundation representative 1' and Nicola Henry highlighted the need to hear victims' experiences when engaging with the OESC. No victims were approached for interview, and this is explained in section 3.6 as a limitation of the study. 'Alannah & Madeline Foundation representative 1' and Nicola Henry explained how it is

very hard to know whether the OESC is effective in its processes of removal as only a victim who has directly engaged with a process would know.

> After they enter onto that (IBA portal) they become the Office of the eSafety client, so they are not our client. So, we don't know their satisfaction levels or what happens as there is a privacy aspect issue. ('Alannah & Madeline foundation representative 1')

However, an insight into victims' experiences was provided by Helen Campbell from Women's Legal Service NSW. Helen Campbell explained that feedback they have received from victims of IBSA who they have referred to the OESC is positive:

> The feedback we're getting is that that our clients are satisfied with that result. (Helen Campbell)

3.6.2.5 The importance of an alternative route

Nicola Henry, Helen Campbell, and Nicolas Suzor highlighted the importance of the OESC as it acts as an alternative avenue of redress for the removal of harmful content as opposed to a criminal approach or a traditional civil approach. Nicola Henry explained that seeking assistance through the criminal justice system is not always the most suitable option for victims of sexual violence specifically. She explained how victims are reluctant to go through the court process as they suffer re-traumatisation. She also pointed out that the IBA portal allows victims to seek removal without having to engage in a court process in person:

> A key finding in much feminist research on sexual violence is that a lot of victims survivors struggle with the criminal justice system. That they experience re-traumatization through the court process. That they suffer unfair cross-examination by defence lawyers' . . . And so with the civil penalty scheme it does offer an alternative for some victims who don't wish to pursue the perpetrators in court. It also offers them the opportunity to have content removed. (Nicola Henry)

Helen Campbell also highlighted the importance of the OESC as she believes the OESC is a much better response over traditional civil approaches due to issues of expense:

> The eSafety Commissioner is a phone call away. It's free. (Helen Campbell)

Nicolas Suzor had a similar view, but he focused on how the OESC provides an alternative route for victims who are unable to articulate their concerns to platforms. He

further explained that a body like the OESC has greater impact than an individual when approaching a platform with a removal request:

> It's helpful to have a more powerful external body like the eSafety commissioner or like an ombudsman or something like that, that can help to prioritize the attention or direct the attention of the platforms. (Nicolas Suzor)

The provision of an individual complaints mechanism by the OESC provides an alternative or supplementary avenue of complaint and redress for victims in addition to the criminal process or traditional civil approach. Criminal and civil approaches can be time consuming, costly (in the civil context), and re-traumatising. Furthermore, the OESC provides an alternative route for victims who are unable to articulate their concerns to platforms or are struggling in their interactions with platforms. The OESC has greater impact than an individual when approaching a platform with a removal request. The Irish regulatory response must consider the inclusion of an individual complaints mechanism therefore ensuring the provision of a fast, free, and less invasive avenue of redress for victims of IBSA.

3.6.2.6 The symbolic role of the Office

Irrespective of the OESC's actual results and impact, Nicola Henry revealed that the mere presence of the OESC plays a symbolic role as it takes responsibility away from victims and shows society that the Government is taking action and that perpetrators will be held accountable. This, in turn, may prevent future perpetrations of IBSA and the posting of harmful online material which supports the view that the OESC is effective in a deterrence role:

> And so I think with a government agency being created it does help to shift some of that burden. And it does shift some of the responsibility back onto the community to take action and to address this issue that we've all created around social media in particular you know digital environments. So there is a symbolic role here as well, the government stepping in and saying yes we're going to take some of that burden. (Nicola Henry)

The OESC plays a symbolic role as it takes responsibility away from victims and shows society that the Government is taking action and that perpetrators will be held accountable. As a result, the mere presence of such a regulatory body has the potential to act as a deterrent to potential perpetrators and can reassure victims that they have a right

to pursue justice. This awareness-raising and deterrent effect has the potential to have a great impact within the Irish context, particularly due to the smaller population and the centralised Governmental structure of the Irish State.

3.6.2.7 Significance of the eSafety Commissioners having a background in the technology industry

Julie Inman Grant is the current eSafety Commissioner. Previous to her appointment, Alastair MacGibbon was the Children's eSafety Commissioner. Both have a background in industry as Julie Inman Grant worked in Microsoft and Alistair MacGibbon worked in eBay. Christiane Gillespie-Jones from Communications Alliance highlighted that the OESC and its functions are effective and work well due to the Commissioner's understanding of industry. As a result, Christiane Gillespie-Jones has suggested that the experience and expertise of the eSafety Commissioners has resulted in a high level of cooperation by industry, particularly by the large social media platforms. Therefore, one view is that the high level of cooperation of the platforms with the eSafety Commissioner could be partially attributable to the Commissioner's experience in the industry. Christiane Gillespie-Jones suggests that one of the reasons that the OESC currently works well is because 'its leader' comes from an industry background and if this was to change, it could be a different story:

> A lot depends on the person who runs the office and Julie comes from industry. She has an industry background. She was in Microsoft before and she has run this office very effectively and efficiently, as did her predecessor, Alastair MacGibbon. But it remains to be seen how someone would run the office if someone was far less inclined to work with industry and to collaborate. (Christiane Gillespie-Jones)

However, while not mentioned by the interview participants, it could be argued that the Commissioner's industry background has led to the eSafety Commissioner focusing too much on collaboration and as a result is not sufficiently independent. Ireland must consider the Australian experience – in addition to its own experience with regulatory bodies like the Data Protection Commissioner – when recruiting for an Online Safety Commissioner.

3.6.3 Theme 3: Considering the appropriateness of the OESC expanded powers

This theme centred on the general rights and obligations associated with the processes of removal by the OESC under the systems in place at the time of the interviews. In particular, this theme questioned the appropriateness of the OESC's expanded powers under the civil penalty regime and whether the OESC is equipped to establish whether content is harmful and should be removed upon request. The key aim of this theme was to consider any issues of free speech and due process that may arise in the context of the OESC's powers and processes. Two sub-themes developed from the data collected under this pre-established theme as follows: freedom of expression and due process.

3.6.3.1 Freedom of Expression

The general consensus of the interview participants was that the removal of harmful content such as intimate images is an acceptable infringement upon free speech where appropriate limitations and processes are in place.

Many justifications for why the removal of harmful content such as intimate images does not_violate freedom of expression were provided by interviewees. These included that freedom of expression is not an absolute right, the importance of a victim-centred approach, and how the OESC targeted approach minimises interference with freedom of expression. However, there was an argument made for a more holistic approach to freedom of expression in Australia. Furthermore, suggestions were made as to why this debate did not feature as a barrier to the establishment of the OESC as compared to what might arise or has arisen in other jurisdictions. There was also an argument made for the need for strict procedures and regulation around how material is removed.

Freedom of expression is not absolute

'Anonymous interviewee 1' acknowledged that the removal processes of the OESC technically infringes upon freedom of expression however the right to freedom of expression is not absolute:

> They by necessity infringe on freedom of expression and as we all know freedom of expression is not absolute. ('Anonymous interviewee 1')

'OESC representative 2', Christiane Gillespie-Jones, and Bianca Fileborn further acknowledged that the right to freedom of expression is not absolute, and a violation may be justified in cases where content causes harm. 'OESC representative 2' noted that there

have always been exceptions to this right and that freedom of expression does not constitute the freedom to cause harm.

'Anonymous interviewee 1' noted that if freedom of expression is violated in cases of IBSA, it is justified by Article 19 of the Universal Declaration of Human Rights and Article 19 of the International Covenant on Civil and Political Rights:

> I think that the way in which the Parliament has set a bar for very harmful content to the extent that it impinges on anyone's freedom of expression I think is justified by reference to international human rights law. It's a very complicated way of saying I haven't seen there yet to be an infringement of freedom of expression. ('Anonymous interviewee 1')

'Anonymous interviewee 1' further related this argument to Ireland explaining that Ireland could follow the Australian approach as the European Convention on Human Rights is similar to the UDHR and the ICCPR:

> I think the approach that we've tried to take without a Human Rights Act has been to look at the requirements of international human rights law and so the European Convention is very similar to the articles . . . So I think you can kind put the US to one side, but if you are comparing Ireland to Australia, I wouldn't have a concern because of the European convention. ('Anonymous interviewee 1')

However, Christiane Gillespie-Jones from Communications Alliance explained that it may be difficult to identify the line between free speech and harmful speech:

> It's the fine line between hate speech and freedom of speech. And Australia struggles greatly with it and Australia always struggles greatly with all of these questions because Australia doesn't have a Bill of Rights. (Christiana Gillespie-Jones)

However, she further explains that in the context of intimate images, this is not as grey an area. As a result, she does not view the removal of intimate images by the OESC as a violation of free speech:

> I think that the sharing of images is a bit easier and the prosecution of it and the judgment call….I conclude, at least at the moment, that the potential infringement on freedom of speech that people could perceive is happening with sharing with the civil parties regime and sharing intimate images. It's not an issue. (Christiana Gillespie-Jones)

Bianca Fileborn further supported this view stating that she believes the freedom of expression argument is often used to facilitate abusive male behaviours against women. She believes the posting of intimate images is not a form of expression as it is not an artistic output:

> I think freedom of expression is often used as an excuse to uphold the rights of men, the interests of men who are engaging in abusive behaviour . . . to me that behaviour either implicitly or explicitly is aimed at controlling and abusing and hurting another person. That's not a form of expression that we have. (Bianca Fileborn)

Importance of a victim-centred approach

Bianca Fileborn explained that the eSafety removal processes must be a 'victim-centred approach'. She explains that these processes are not aimed at punishing a perpetrator but rather about removal of harmful content. As a result, the victim needs to be the priority when considering what should be removed. This view was articulated by Bianca Fileborn who stated that protecting the victim is regarded as a greater priority than protecting a potential infringement of free speech:

> It's not a criminal standard of proof. It's about taking an image down. So, I think it needs to be based on what the victim is saying. (Bianca Fileborn)

Targeted approach minimises interference with freedom of expression

The targeted approach of the OESC – where only the reported harmful content is removed and not any surrounding or associated content – reduces the risk of potential freedom of expression violations. Content which is posted alongside the harmful content or on the same platform may not be harmful and therefore the removal of such content would be likely to raise freedom of expression issues.

> We remove only that content which is reported to us as offending for instance like particularly URLs not a whole domain or website. ('OESC representative 1')

Ireland must consider strict removal procedures around the selecting of content for removal once reported, so to reduce the risk of FOE violations.

Holistic approach and other thoughts

Christiana Gillespie-Jones from Communications Alliance highlighted the general need for a more 'holistic debate' around the issues of harmful online content and free speech issues in Australia. Although this debate has gathered momentum in Ireland,[53] there has been a lack of discussion within the Australian context. 'OESC representative 3' explained that there was little consideration of free speech issues when the OESC was being established. A potential reason given for this was that, compared to Ireland, Australia does not have constitutional protection for the right to free expression.

Nicolas Suzor presented another line of thought when considering whether the OESC hinders freedom of expression. Nicolas Suzor explains that the implementation of Governmental penalties to remove online content tends to create a system of 'uncertainty'. This results in platforms acting on the side of caution therefore removing content which might be legitimate which results in potential violations of freedom of expression. Nicolas Suzor acknowledges the need for harsh penalties in order to achieve compliance. However, he further recognises the need for due process safeguards to ensure that harsh penalties are implemented correctly. Without the necessary safeguards, a civil penalty regime may not be appropriate as it may infringe on freedom of expression. As a result, Nicolas Suzor suggests 'a soft approach may be appropriate in some circumstances.' However, Section 220A of Online Safety Act 2021 now requires the OESC to develop an internal review scheme to allow for the review of decisions made by the OESC. This allows for a due process safeguard as noted by Nicolas Suzor.

In summary, harsh penalties may create a system of uncertainty for social media providers. As a result, penalties must be backed by due process safeguards so to prevent the removal of legitimate content. Previously, there was a lack of safeguards under the legislation in place at the time of the interviews, however, the Online Safety Act 2021 developed an internal review process which allows for a review of decisions made by the OESC. Ireland must ensure safeguards are in place alongside any penalty systems. An internal review process provides such a safeguard.

3.6.3.2 Due Process

[53] Kevin Doyle, 'Facebook Warns Digital Safety Commissioner 'Could Limit Freedom of Expression' *Independent* (Dublin, November 2018); Facebook Ireland Limited, Public Consultation on the Regulation of Harmful Content on Online Platforms and the Implementation of the Revised Audiovisual Media Services Directive (27 June 2019); Stephen McDermot, Facebook Urges Against 'Punitive' Fines for Firms who Breach Government's New Online Safety Laws (*The Journal*, June 2019) < https://www.thejournal.ie/facebook-submissions-irish-government-safety-act-4699145-Jun2019/ > accessed 24 February 2022.

Information collected from the interviews presented a mixed view on whether the OESC's processes of removal provide adequate due process. In particular, there were many views on whether the civil penalty regime and the power of imposing fines for non-compliance satisfied a suitable level of due process.

As discussed in Chapter 2,[54] the OESC can issue a removal request and can also enforce a civil penalty provision as set out under part 4 of the Regulatory Powers (Standard Provisions) Act 2014 for non-compliance with a request. The OESC can execute a civil penalty by means of an infringement notice, an enforceable undertaking, or an injunction.

Peter Clarke and Helen Campbell discussed how the OESC powers under the civil penalty regime do not hinder due process. They both justified this view by stating that the courts are involved in issuing an order and decisions are reviewable. 'OESC representative 1', 'OESC representative 2' and 'OESC representative 3' also endorsed this view. However, an infringement notice does not require a court order and relies solely on the judgement of the OESC. 'OESC representative 1' justified this view by explaining that a decision to impose an infringement notice can be challenged:

> Not judicial review, administrative review. It's an administrative decision and there is a check and that is that the person or the entity they can apply to the Administrative Appeals Tribunal for review of our decision to give a removal notice or not to give one. ('OESC representative 1')

Peter Clarke highlighted the need for the courts to ensure due process:

> So, in my view look the process is ultimately bureaucratic and it's court driven as it should be. You know you can't have government authorities slapping large fines on individuals being judge jury and executioner. They've got to have a role which is prosecuting a claim and let a court decide. (Peter Clarke)

However, Peter Clarke highlighted that ensuring due process may bring other challenges. Peter Clarke highlighted that the court process is bureaucratic and the process of the OESC obtaining an order can take significant time. As a result, the intimate image may be further disseminated by the time an order is received. As of yet, the OESC has not applied for a court order under the civil penalty regime. Therefore, this challenge has not yet occurred in practice. However, empowering the OESC with powers to make a determination on whether a piece of content meets a harmful threshold and should be

[54] See Chapter 2 section 2.3.8.2.

removed which can later be appealed to a court may reduce the bureaucratic process of seeking a court order therefore reducing the time frame in which the content may rapidly spread.

Nicolas Suzor stated that under the legislation in place at the time of the interview the OESC is not making a 'legal determination' on what content should be removed. Instead, they are investigating a report about a particular piece of content and then are 'having a conversation with the platform' who either 'agrees or disagrees with their assessment' on whether to remove the content. Nicolas Suzor explained that while certain harmful material is well defined and easy for platforms to identify, such as child sexual abuse material, other harmful content is not so easy to define. Therefore, a more empowered regulator with the expertise to make a determination on what is harmful or not may be beneficial due to the complex process of identifying what material is harmful and should be removed. Nicolas Suzor 'would rather see a more empowered regulator that is required to abide by due process and make a binding determination and you can back that by a penalty.' Therefore, Nicolas Suzor suggested that the possibility of giving greater legal power to the OESC should be considered. Under the legislation at the time of the interview and the current Online Safety Act 2021, if the OESC makes a determination that a piece of content is harmful and the social media platform disagrees and refuses to remove, the OESC needs to apply for a court order to direct the platform to remove the content. It could be more appropriate if a body with the expertise to make a determination (such as the OESC) was empowered to make such a decision so to ensure qualified decisions are being made which can later be reviewed by a court should a dispute arise over the removal of legitimate content.

The Irish regulatory response must be designed in order to ensure due process and to achieve the goal of removing harmful content in an effective manner. While the interviews indicate that the OESC provides due process as the courts are involved in granting orders for injunctions, civil penalties, and enforceable undertakings, the interviews also suggest that these processes can lead to delays that can hinder the OESC ability to address the immediacy and scale of distribution in the online sphere. As a result, in order to respond effectively to the nature of the online environment and the particular nature of IBSA, the Irish regulatory response must consider an empowered regulator that can make a legal determination than can later be reviewed by a court therefore achieving a balance of effective enforcement with due process safeguards.

Another issue raised during the interviews by two participants was the lack of transparency in the decision-making process by the OESC on what material meets the definition of 'intimate image',[55] 'cyberbullying material'[56] or 'prohibited content'[57] and should be requested to be removed once reported. Bianca Fileborn specifically highlighted the lack of information around the OESC's 'fact-finding steps' and the 'standard of proof' that they work towards. 'Anonymous interviewee 1' stated that it is unknown how the OESC protects due process rights.

'Alannah & Madeline Foundation representative 1' suggested that a clear definition of harmful material would provide a standard upon which the efficiency of the OESC's decision-making processes for removal could be assessed. 'Alannah & Madeline Foundation representative 1' explained that Australia does not have a clear understanding on what constitutes harmful material. This same interviewee suggested that Australia needs to debate their 'level of tolerance and how things evolve and change' in the context of harmful material. 'OESC representative 1' advised that Ireland should take inspiration from New Zealand's definition of harmful content under the harmful communications legislation. 'OESC representative 1' confirmed they have not 'gone down that path'. 'OESC representative 3' also acknowledged that there is a need for clear standards and definitions from a global perspective:

> You'll know that there is a wider global policy debate in relation to this in the UK and France on harmful content. And I think from, and I am not speaking from an Australian Government perspective, but from a global perspective there is a need for clearer definitions and thresholds just for clarity for the general public and for industry to be able to take action so having broad based kind of definitions but with kind of clear thresholds of action is considered maybe towards best practice. ('OESC representative 3')

3.6.4 Theme 4: The intermediary debate

The purpose of this theme was to allow interviewees to give their opinion on the role of intermediaries and the value of intermediary self-regulation. Opinions, comments, and views gathered during the interviews under this theme can be summarised into four broad categories as follows: self-regulation is insufficient, the OESC enhances self-regulation,

[55] Enhancing Online Safety Act 2015, s 9B as amended by the Enhancing Online Safety (Non-consensual sharing of intimate images) Act 2018.
[56] Enhancing Online Safety Act 2015, s 5.
[57] Broadcasting Services Act 1992, Schedule 7 Clause 20 & 21.

statutory power is only necessary when self-regulation fails, and the OESC is not a barrier to self-regulation.

3.6.4.1 Self-regulation is insufficient

During the interviews, all interviewees acknowledged that relying solely on industry self-regulation in the context of harmful online content and the removal of such content is insufficient. Helen Campell stated that 'self-regulation doesn't work', while Peter Clarke described self-regulation as a 'waste of time'. While DIGI, as mentioned in Chapter 2, highlighted the need for less regulation due to successfully established self-regulatory processes, the interviewed industry representative Christiane Gillespie-Jones from Communications Alliance noted how regulation did not deter their self-regulatory processes. Bianca Fileborn believes intermediaries do a 'terrible job of self-regulating' as their goal is to make profit and that this cannot be achieved by 'strictly regulating platforms'. Bianca Fileborn justified her opinion by pointing out that self-regulation has been insufficient in the past. She demonstrated this through an example of abuse against high profile feminist commentators in Australia who reported abusive material and were told that the material does not violate community standards. When they went to highlight the abuse through the site by means of capturing images of the abusive messages, they were told this was a breach of the platform's privacy standards. Bianca Fileborn also highlights the difference in motives and the ineffective nature of intermediary community standards/policies:

> So they have community standards in place but they're often incredibly low and insufficient and incredibly gendered in terms of how they're actually operationalized . . . Most of these platforms are based on very kind of Western liberal masculine ideas of free speech and the freedom to do almost and say whatever you like. (Bianca Fileborn)

Furthermore, some participants highlighted the challenges in assessing whether self-regulation is effective. Bianca Fileborn, for instance, noted that there is a lack of transparency about how self-regulation is conducted:

> Are they actually enforced in a consistent way . . . how are those community standards actually interpreted . . . there's also some questions around the actual interpretation and application of the rules and standards in practice. (Bianca Fileborn)

Nicolas Suzor explains how he does not believe that a platform can make decisions which historically would be made by a judge, or at least an empowered regulator. Therefore, he questions the effectiveness of self-regulatory policies:

> We would historically expect a judge to be making that call or at least an empowered independent regulator who is bound by the obligations of administrative law and natural justice and whose decision you can appeal to a tribunal, at least if not a court. Those are the sorts of decisions that I don't really trust a platform to make on their own. (Nicolas Suzor)

However, Nicolas Suzor does acknowledge how current self-regulatory regimes against IBSA seem to work well due to the high-profile nature of the topic:

> Having said that, image-based abuse is really interesting because it's such a pointed issue, all the commercial platforms have had to take it seriously. They are so worried about regulation that they are willing to develop quite good self-regulatory approaches. And so in this specific case, we might say that the self-regulatory approach seems to be working kind of well. I don't hear a lot of complaints about it so far. I think because this is such a high-profile hot topic issue that the platforms can't afford to drag their feet. (Nicolas Suzor)

Overall, the interviews supported the view that self-regulatory policies have historically failed in Australia and as a result the establishment of a regulatory body with adequate investigation and enforcement powers was necessary.

3.6.4.2 The OESC enhances self-regulation

Three interviewees highlighted the view that the OESC is a necessity and facilitates the execution of sufficient self-regulatory policies. ‘Anonymous interviewee 1’ explained that strict regulation and oversight reduces the need to enforce the law against intermediaries as they tend to implement more efficient self-regulatory policies in response to strict regulation.

> I think the eSafety Commissioner is a necessity . . . The irony is that the better the regulator is, a regulator like the eSafety Commissioner, the more effective they are, in a sense sometimes the less they have to do. And it's a good thing because it encourages the various companies to self-regulate more effectively and more diligently and more rigorously. And so in the end, if you want to believe in a self-regulation system, you need to have that additional layer of oversight. (‘Anonymous interviewee 1’)

Nicolas Suzor explained that 'they [intermediaries] are so worried about regulation that they are willing to develop quite good self-regulatory approaches'. Nicolas Suzor also pointed out that once regulation is in place, intermediaries do not want to be seen to be penalised as it tarnishes their reputation. Therefore, Nicolas Suzor explained that it is the 'threat of losing legitimacy that makes self-regulatory regimes effective' also.

Helen Campbell explained how regulation leads to more cooperation and it gives companies a 'level playing field' as all must abide by the law. Therefore, she argues that self-regulatory policies become more effective when there are laws in place which impose responsibility on all intermediaries:

> Regulation works and you get a higher level of voluntary compliance with regulation from a major corporation . . . And if they're confident that all their competitors have had the same compliance cost as they do, hey, level playing field. So why would you bother exposing yourself to risk. You're on the same playing field as your competitors . . . They are not trying to make trouble they are just trying to make money. (Helen Campbell)

This suggests that the establishment of an empowered regulator in Ireland has the potential encourage the development of more robust safety policies and reporting mechanisms by online service providers.

3.6.4.3 Statutory power is only necessary when self-regulation fails

'Alannah & Madeline Foundation representative 1' believes platforms are very responsive and therefore they advise victims to first approach the platform for removal before the OESC, which shows some support for self-regulation. However, 'Alannah & Madeline Foundation representative 1', acknowledges that there is a need for regulation for when self-regulation fails:

> What we tell everyone is approach the provider of the platform first because most things can be resolved. In our experience mostly the companies are very responsive and responsible. So, I want to be really clear. It's really important that we don't say as soon as there is a problem you need to go to the Office of the eSafety and evoke that route first. ('Alannah & Madeline Foundation representative 1')

Overall, the findings from the interviews suggest that the main social media providers respond to complaints made through their own reporting systems in an effective manner. Notwithstanding this, the existence of a robust statutory alternative likely increases the importance placed on those internal systems within the priorities of the social media

providers. Notwithstanding the generally effective operation of these systems, the regulatory system plays an important role where internal systems fail. Moreover, certain smaller 'rogue' platforms and pornography websites have been less responsive to concerns regarding IBSA and this reaffirms the importance of a regulatory body with statutory powers.

3.6.4.4 The OESC is not a barrier to self-regulation

Views expressed by five participants revealed the importance of compliance and how the fostering of good relationships between the OESC and industry is essential when developing a collaborative approach to the regulation of the internet. 'OESC representative 1', 'OESC representative 2', and 'OESC representative 3' explained how the fostering of good relationships with industry is essential. As a result of their good relationships, they have received high levels of compliance with their requests and self-regulation policies by the major companies are in line with regulatory standards.

> What surprised us though is like the level of cooperation we've managed to garner from all types of websites. ('OESC representative 1')

'OESC representative 2' also highlighted that their lack of need to use their formal powers under the penalty regime is perhaps a reflection of the good rapport that they have built with industry which has led to stronger self-regulatory policies. However, 'OESC representative 1' acknowledged that 'those kinds of self-regulatory steps were only taken by particular platforms and they're not the platforms where we find most of the live content'. Christiane Gillespie-Jones from Communications Alliance talked about how the OESC is not a barrier to how they operate and that the regulation and powers of the OESC does not deter them from still developing self-regulatory policies and standards. Under the Telecommunications Act, Communications Alliance have been granted the power to create and maintain the codes, standards and guidelines by which the telecommunications industry operates. However, Christiane Gillespie-Jones stated that Communications Alliance have not sought to develop codes of practice in the area of IBSA:

> We have not sought to self-regulate in, for example, the area of sharing of intimate images, but we do self-regulate in other areas and the eSafety commissioner so

> far has not been our difficulty . . . we haven't perceived her office as an obstacle to self-regulation. (Christiane Gillespie-Jones)

This is in contrast to the view expressed by DIGI as outlined in Chapter 2 whereby DIGI stated that regulation hinders the development of self-regulatory policies and practices.

Christiane Gillespie-Jones observed that pressure from the OESC may be useful:

> We do want to definitely maintain our self-regulatory regime, but I don't see a need to exclude each other. To a certain extent the additional pressure from an eSafety commissioner, but also the function that she fulfils in terms of education and with cyber bullying and especially the sharing of images in that area, I think it is very useful to have an office like hers. And I don't think that we would say we should go necessarily without. I wouldn't know, frankly, back then whether we were hugely in favour of the establishment of an eSafety Commissioner. Having said that, at the moment, we are not unhappy with the existence of the office. (Christiane Gillespie-Jones)

Furthermore, 'Alannah & Madeline Foundation representative 1' identified 'balance' as important and suggested that the promotion of cooperation and collaboration should be given priority over enforcement.

> I get it as a last resort I really do but the most important thing is to encourage compliance. That's the most important thing. ('Alannah & Madeline Foundation representative 1')

In summary, the OESC establishes good collaboration and cooperation with service providers and therefore is not viewed as a body to work against. As a result, the OESC has not deterred service providers in engaging in the development of policies and technologies to protect users on their platforms. Indeed, as argued above, the existence of a robust statutory regime is likely to encourage the development of effective and well-resourced internal review and complaints systems.

3.6.5 Theme 5: Improvements

Matters identified under this theme related to any problem areas the interviewees perceived as related to the OESC, successes of the OESC, and suggestions on how the OESC could improve. Four sub-themes developed as follows: visibility, funding and resources, collaboration with NGOs, and the OESC as a separate entity.

3.6.5.1 Visibility

Four participants expressed an opinion that there is a lack of awareness of the OESC and that it would benefit from increased visibility. Interviewees explained that people need to be aware of the OESC without having a 'specific reason for knowing about the Office' or looking for the Office. Peter Clarke and Bianca Fileborn stated that they would not know about the body but for 'working in the field' of online regulation. Peter Clarke explained that their visibility is mainly within 'industry' or with 'people who float around in the area of privacy and these types of issues'. 'Alannah & Madeline Foundation representative 2' and 'Alannah & Madeline Foundation representative 3' also experienced a low level of knowledge about the eSafety Commissioner in school settings suggesting that 'schools don't even know that they exist' and that they 'constantly get blank looks from especially parents and teachers'. 'Alannah & Madeline Foundation representative 2' further explained that there is a lack of awareness for federal bodies in general in Australia and suggested that this may be a possible reason for the lack of awareness for the eSafety Commissioner:

> It has a bit of a PR challenge I think because it is a federal body. Whereas how Australia is, a lot of people know things on a state level but they're not quite sure of things on a federal level. ('Alannah & Madeline Foundation representative 2')

It is less likely that this issue would occur in the Irish context due to Ireland being smaller geographically and in population. Furthermore, as Ireland has a unitary system of government as opposed to a federal system, there are less layers within the political structure which leads to greater awareness of regulatory bodies.

3.6.5.2 Funding and Resources

Another suggested improvement suggested by four participants was a need for increased funding and resources. Bianca Fileborn discussed how the OESC is tasked with a complicated and technical job which needs to be supported with an appropriate level of funding in order to be fully effective. Bianca Fileborn believes the OESC's current funding could be increased:

> I get the sense that they're vastly underfunded so it would be fantastic for them to actually get the funding that they need to properly do all the things that they need to do to address what is a deeply complex and challenging issue. (Bianca Fileborn)

‘OESC representative 1’ and ‘OESC representative 2’ suggested they would like to offer victims another avenue to communicate with the OESC via a text messaging service.

> We would like to be able to offer people another way to communicate with us which is SMS. We think there's a real place for it especially with younger people. So, some sort of text-based service. We would like to do that. (‘OESC representative 1’)

‘OESC representative 1’ and ‘OESC representative 2’ also identified an issue with recording time frames of content removal. Currently, the OESC has no way to monitor how long it takes to remove harmful content from when the initial report is made to when the content is removed. ‘OESC representative 1’ stated that this process can take anything from ‘half an hour to a few days’ depending on if they have to go down the track of identifying administrative contacts through hosting providers. The current system they have is manual. In order to track that information, they would need an IT system to support it.

The funding of the Irish regulator will be a critical issue and Ireland can learn from both the experience of the OESC but also from its own experience of inadequately funded regulators such as the Data Protection Commissioner.

3.6.5.3 More collaboration with NGOs

Overall, interviewees agreed that the OESC has fostered good relationships and collaboration with intermediaries and industry. However, ‘Alannah & Madeline Foundation representative 1’ believes the OESC could link more with non-governmental organisations. This same interviewee discussed how ‘initiatives, policies, activities, programs, information, and education are too disjointed’ and that there is a lack of ‘common understanding’.

> They basically run their own self as a government, and they let NGOs do their own thing. It’s annoying to me. I think there is a gap at the moment around the way we are doing this work. (‘Alannah & Madeline Foundation representative 1’)

Furthermore, email correspondence with ‘Alannah & Madeline Foundation representative 1’ highlighted that although the Alannah & Madeline Foundation is a ‘Trusted eSafety Provider’, the Foundation has received ‘few referrals’ from the OESC. When the OESC first commenced the Trusted eSafety Provider Scheme, the Alannah &

Madeline Foundation received ‘a lot of referrals’ but ‘gradually’ the OESC took on the role of working with schools and providing free resources. While the Alannah & Madeline Foundation still receive requests from schools, ‘Alannah & Madeline Foundation representative 1’ stated that was due to their ‘own marketing in most cases.'[58]

‘Alannah & Madeline Foundation representative 2’ suggests how greater collaboration with NGO’s would benefit the OESC as NGOs can be more direct in their messaging:

> They're a government agency so they're quite limited by what they can say and what their advice is and what their approach is. I think one of the benefits we have as a non-government agency is that we can be a bit more frank or more direct in our conversations than the office can be. (‘Alannah & Madeline Foundation representative 1’)

In summary, while the OESC has fostered good relationships and collaboration with intermediaries and industry there is a need for greater collaboration with NGOs around the provision of activities, programs, information, and education. This would create a more unified approach to education and a clear message to target audiences.

3.6.5.4 The OESC as a separate entity

As explained in Chapter 2, the OESC is under the umbrella of the ACMA and remains within the structure of the ACMA under the Online Safety Act 2021. While the OESC makes its own decisions, both share funding and resources. ‘Anonymous interviewee 1’ and ‘Anonymous interviewee 2’ highlighted a view that the OESC should be a separate entity from the ACMA. ‘Anonymous interviewee 1’ also revealed that there is a lot of overlapping of processes between the OESC and other organisations which makes the system complicated. For example, the OESC is not the only organisation who provides support for online safety. The Australian police, intermediaries, and NGOs also provide various supports such as reporting mechanisms and educative campaigns.

‘Anonymous interviewee 1’ questioned whether the OESC is best as a single entity or combined with another body. The participant explained that many issues overlap with other organisations and sometimes it is better to look at issues through a broader outlook i.e. through an organisation who is equipped to considered multiple issues. However, the interviewee identified that the body could become overloaded. If the body is a single

[58] See email correspondence with ‘Alannah & Madeline Foundation representative 1’ on file with author.

entity, then it must foster good relationships with other bodies in similar areas to work effectively together.

> The decision to make it its own entity. I wonder whether that is something that would be worth revisiting because so many of these issues do overlap . . . If you establish it as its own separate entity, then I think it would be useful to think very deeply about how that body can operate most effectively with other bodies that exercise similar sorts of functions and powers and responsibilities like violence and human rights issues. ('Anonymous interviewee 1')

'Anonymous interviewee 2' suggested that the OESC should have increased powers separate to the ACMA. This interviewee justified this by stating that there are issues between the ACMA and the OESC which causes tensions. These issues appear to stem around resourcing, budget decisions, and responsibility:

> I don't think that's necessarily a happy relationship. I think there are a lot of interdepartmental tensions between the ACMA, the department, and the eSafety Commissioner. And I think that manifests around resourcing and budget decisions as well as growing responsibility for other things. ('Anonymous interviewee 2')

The interviewee explained that the ACMA had authority over content regulation, but that the OESC now have more specialised staff to deal with these issues. Therefore, he/she observed that empowering the OESC would mean decreasing the power of the ACMA which is an area of tension:

> The ACMA has historically had quite a lot of responsibility for content regulation. Increasingly, it seems like the eSafety Commissioner, the office has specialist staff that are better placed to deal with a lot of these issues. And so some people would want to increase the power of the eSafety Commissioner, but that necessarily comes at the cost of the power of the rest of the ACMA. And I understand informally that there is a bit of a power struggle going on there. ('Anonymous interviewee 2')

The participant suggested that more independence for the OESC would be welcomed:

> So if I were going to look at increasing the power of the eSafety Commissioner, I would also want to increase its financial and administrative independence. So, I would like to see an increase in that sort of, particularly the ombudsman role negotiating between citizens and platforms, but I would like to see more independence. ('Anonymous Interviewee 2')

The interviews suggest that the OESC would benefit from a single entity structure. Consequently, Ireland should consider a single entity structure however such a body must

foster good relationships with other bodies with relevant powers so to ensure effective collaboration when issues overlap.

3.7 Issues highlighted in the interviews that have been modified by the Online Safety Act 2021

Following the conducting of the interviews, the Online Safety Act 2021 was passed as outlined in Chapter 2. Some of the issues highlighted during the interviews were impacted by the new legislation while others remain unchanged. This section identifies issues which were highlighted under the various 'Themes' which have now been affected due to the new legislation. Below is a summary of these key changes relevant to IBSA in the context of 'Theme 2' and 'Theme 3'. Issues raised under 'Theme 1', 'Theme 4', and 'Theme 5' remain unaffected by the new legislation.

3.7.1 The impact of the Online Safety Act on issues highlighted in 'Theme 2' in the context of image-based sexual abuse

'Theme 2' discussed how the OESC can never permanently remove an image and that content hosted overseas and through rogue websites will remain a problem when combating IBSA through the Enhancing Online Safety Act 2015 as amended by the Enhancing Online Safety Act (Non-consensual sharing of intima images) Act 2018. The provision of link deletion notices under Section 124 of the Online Safety Act helps to mitigate these issues. While the OESC cannot guarantee the removal of an image, it is now given power to not only request the removal of the access to a link through a search engine provider but can now enforce it through a civil penalty. In a situation whereby a website hosted overseas does not remove harmful content as requested by the OESC or whereby the OESC cannot identify the host/poster of the intimate image, it can instead reduce access to the content through a link deletion notice not previously provided for under the Enhancing Online Safety Act 2015. 'Theme 2' also discussed how the rapid speed in which material can spread online can cause issues when combating IBSA and as a result there is a need for definite timeframes upon which removal notices should be executed. The new legislation under the Online Safety Act now requires the recipient of a removal notice to remove the content within 24 hours.

3.7.2 The impact of the Online Safety Act on issues highlighted in 'Theme 3' in the context of image-based sexual abuse

'Theme 3' discussed how the OESC must practice strict procedures around identifying what reported content warrants a removal notice. The new legislation provides a more detailed definition of an intimate image under Section 15 which provides the OESC a clear standard to refer to when assessing whether a reported image requires removal. 'Theme 3' also discussed how the legislation governing the OESC must include due process safeguards so to ensure notices and penalties issued by the OESC are implemented fairly. The legislation at the time of the interviews did not require the OESC to provide an internal review process of decisions should an end user or service provider wish to challenge such a decision without having to go to Court. However, Section 220 of the Online Safety Act requires the OESC to establish an internal review process to ensure decisions made are made fairly.

'Theme 3' discussed the need for greater transparency around the practices of the OESC. While the legislation at the time of the interviews obliged the OESC to release an annual report, the legislation did not set out specific requirements regarding the type of data to be included in the report. Section 183 of the new legislation provides a list of data which must be included in the annual report as set out in Chapter 2.[59] The requirement to report on specified data aims to ensure greater transparency.

3.8 Limitations of the interview process

Following reflection on the interview process, four main limitations are identified: small sample size, no representation from the category of online intermediaries, the absence of victim's perspectives, and the subsequent passage of the Online Safety Act in 2021.

Interview data is sometimes criticised because of the presumed lack of objectivity due to the use of a relatively small sample size.[60] This study utilises a relatively small dataset in terms of the interviews conducted. This is due to a lack of agreement by potential participants to engage with the study. Furthermore, the participant category of 'online intermediaries' is not represented. This is due to the fact that they declined the invitation

[59] See Chapter 2 section 2.5.3.9.
[60] Lisa Webley, 'Qualitative Approaches to Empirical Legal Research' in P. Cane & H. Kritzer (eds) *The Oxford Handbook of Empirical Legal Research* (Oxford University Press, 2010) 930; John W. Cresswell, *Research Design: Qualitative, Quantitative, and Mixed Research Methods* (Sage, 2013).

to participate. While the author acknowledges the limitations, the interviews provided invaluable insights that supplement the desk-based research. The answers given to interview questions in this research are not used as the sole basis upon which to base any argument. The interviews assisted in the providing of context, local insight, and helped to challenge the narrative that emerged from the other sources.

Even though this chapter focuses on the legal processes in place in Australia, the perspectives of victims who directly engaged with the OESC's processes of removal would be beneficial. After careful consideration, the author opted to focus on non-vulnerable parties that have interacted with the OESC system. From an ethical perspective, interviewing victims of IBSA risks causing harm by unearthing past vulnerable experiences. Furthermore, even in the absence of the ethical considerations, it was deemed to be unviable in the context of this Ph.D project to identify and access Australian-based victims for the purposes of interview.

The passing of the Online Safety Act 2021 may be viewed as a limitation of this research as the interviews were based on a system operating on a legal basis that has now been updated. While many provisions of the legislation in place at the time of the interviews were carried over into the Online Safety Act, there were also some updates and changes. However, in the context of Ireland, there is valuable insight to be gained from the system that was in place at the time of the interviews and a further layer of analysis to be learned from by considering the changes that have occurred due to the new legislation. Both situations — the situation in place under the legislation at the time the interviews were conducted and the situation since the new legislation was enacted — provide valuable lessons for Ireland to learn from.

3.9 Summary of lessons and issues identified to be discussed in Chapter 5

A key aim of this chapter was to identify lessons and issues on the functioning of the OESC under the legislation in place at the time as perceived by experts that could help inform the regulatory response to IBSA in the Irish context. Building from the desk-based research discussed in Chapter 2, the semi-structured interviews discussed in this chapter provide additional insight into the operation of the OESC in practice. Some of the lessons learned from the Australian experience provide clear guidance on the best practice while others flag areas of concern. Both provide Ireland with an opportunity to learn from the Australian experience as discussed in Chapter 5 of this thesis.

Overall, the research conducted in this chapter concludes that the OESC plays a valuable role in the tackling of IBSA and can be regarded, in general, as effective in executing its functions. It provides an important supplementary route for IBSA victims when seeking redress. Limitations to the body's effectiveness remain, however. It is still challenged by issues of enforcement in the online environment such as jurisdictional and anonymity challenges. The OESC's main challenge under the legislation in place at the time of the interviews was removing content which was hosted overseas or on small rogue platforms where it was difficult to identify its administrator. The lack of ability to identify the perpetrator inhibited the ability of the OESC to seek removal either through formal means if hosted within Australia or informal means if hosted outside of Australia and as a result the OESC resorted to an alternative action of reducing the visibility of the intimate image through requesting the voluntary de-indexing of the content by search engines. While these challenges around jurisdiction and anonymity remain, the Online Safety Act 2021 provides support for a useful mitigation measure by empowering the OESC with powers to issue link deletion notices and app removal notices to ensure the reduced access of harmful content within Australia. Below is an outline of the key lessons and issues identified in this chapter which will be used to assess the potential impact of Ireland's enforcement response in Chapter 5.

3.9.1 An empowered regulator

A core strength of the OESC is the ability to impose removal notices and apply for court orders for enforcement actions such as injunctions, enforceable undertakings, or civil penalties. These robust statutory powers ensure that the OESC is seen as an empowered enforcer. While the OESC has not yet imposed penalties for non-compliance with removal notices, the ability to take action enhances the voluntary compliance from intermediaries, social media services, and end-users. Without such power there would be less compliance as seen prior to the OESC's expanded powers. The level of power afforded to an equivalent authority in Ireland will need to be carefully assessed and considered as a similar authority with limited powers may be regarded as ineffective in remedying victims of IBSA.

While the OESC is successful in assisting in the removal of reported intimate images in the majority of cases, there is a need for an intermediate goal for when removal is not possible. In such cases the OESC makes efforts to reduce the visibility of the content by

ordering the removal of the content from search engine results and failure to comply with such an order can result in a penalty under the Online Safety Act 2021. This approach should also be considered in the Irish context. Analysis of the Irish legislation in Chapter 5 will examine whether Ireland has considered an alternative approach for cases where removal of the reported material cannot be guaranteed.

The timely removal of harmful content while ensuring due process standards are met is essential. The Australian experience demonstrates how this can be challenging to achieve in practice. While the OESC aims to remove material in a timely fashion, this is not always achieved due to the recipients of removal notices failing to remove the material in a timely manner. As a result, there were proposals to require the OESC to respond to reports within a required time frame. The Online Safety Act 2021 adopted these proposals and now requires material to be removed within 24 hours of receiving a removal notice.

The OESC currently receives a high level of voluntary compliance from issued removal notices. However, in situations where voluntary compliance is not forthcoming, the need to seek a court order may take considerable time within which the reported intimate image may be widely distributed making it impossible to effectively remedy victims. There is an argument for providing the OESC with additional powers to make determinations to impose a civil penalty without a court order (while maintaining a right to make a court appeal). The Online Safety Act 2021 has not provided for this. Analysis of the Irish legislation in Chapter 5 must examine whether the system balances the protection of legitimate content and due process alongside remedying victims by removing intimate images in a timely manner.

3.9.2 The need for educative and awareness raising functions

The OESC takes both a preventative and responsive–approach to online regulation by fulfilling educative functions in addition to its enforcement role. The OESC provides an array of educational tools and resources to a wide-ranging audience across Australia. These resources aim to educate potential perpetrators, victims, students, family, friends, frontline workers, and bystanders. The education provided aims to reduce the perpetration of online crimes such as IBSA while also providing victims with clear avenues for redress. The establishment of specific codes of practice and standards with which many intermediaries voluntarily comply reduces the potential perpetration of IBSA and other online harmful communications. Some of the interview findings suggest that if a more adversarial approach was adopted with an emphasis on harsh enforcement and little focus

on education or preventative measures, intermediaries may be incentivised to take an overly censorious position and remove legitimate content in fear of receiving a penalty. It is vital that Ireland establishes clear codes of practice and standards upon which it expects online platforms to comply. Discussions in Chapter 5 will establish if Ireland has struck the right balance between preventative and responsive measures.

3.9.3 A Governmental response alone is insufficient, a collaborative approach is essential

The Australian experience has confirmed that while self-regulation alone is insufficient, there is still a place for self-regulation alongside a body providing oversight. Collaboration is an essential practice of the OESC. Working with key national stakeholders in the digital and technology realm in Australia assists the OESC in achieving its goal of providing a safer online environment for Australians. Chapter 5 will consider whether Ireland's equivalent body has established avenues for collaboration with key stakeholders who can contribute to the provision of a safer online environment.

3.9.4 International Collaboration

A key identified problem for the OESC is the removal of content hosted overseas. Within the context of child sexual abuse material, established channels for international collaboration such as with INHOPE are essential for overcoming this issue. However, there is a lack of international collaboration for the removal of other content such as intimate images when hosted overseas. This is particularly an issue for content hosted on pornography sites hosted overseas. Discussions in Chapter 5 need to consider whether Ireland could establish an international collaborative response for the removal of reported material hosted outside of Ireland.

3.9.5 The importance of transparency

There is currently a lack of transparency in the OESC's decision-making processes. Greater clarity regarding the criteria used for the selection and removal of harmful content is desirable. However, the Online Safety Act provides for a more exhaustive definition of an intimate image which will provide clear guidance to the OESC when establishing whether an image meets this threshold of being an 'intimate image'. Furthermore, the Online Safety Act requires the OESC to report on specific data in the Annual reports which will also provide greater transparency into the OESC processes and practices.

Analysis of the Irish proposals in Chapter 5 will consider what reporting requirements are imposed on the Irish regulator and whether any improvements are necessary for the purposes of transparency. Chapter 5 will also consider whether the legislation provides sufficient clarity on the key definitions and legal standards that will be applied.

3.9.6 Independent and adequately resourced body

Ireland must consider whether an equivalent body to the OESC would be best established as an independent body, a body linked with another organisation, or assign the role to an already established body such as the Broadcasting Authority of Ireland. The interviews conducted suggest that the Australian experience has shown that the OESC should sit as an independent body so to avoid disputes over allocation of resources and areas of authority. However, there is also an argument that a single body may become overloaded and may have a broader view if linked to other organisations already in the field of online regulation. The interview findings suggest that the OESC links to the Broadcasting Services such as the Classification Board hinders its ability to carry out its functions in a timely manner. Therefore, Ireland must consider whether linking its body to an already established body is best practice considering the contemporary online environment or whether an independent body is more suitable. Many organisations carrying out similar functions can cause confusion for the general public, including for victims seeking redress.

Due to the technical and complicated job carried out by the OESC, four participants suggested that the OESC required increased funding. Separating the OESC financially from the ACMA may reduce the clashes in funding and may better equip the OESC to allocate finances towards necessary resources. Such resources include the provision of an additional avenue of communication for victims through a text messaging service as suggested by representatives from the OESC. Furthermore, representatives from the OESC highlighted the need for an IT system that would support the timeframe recording of the removal processes from the initial reporting stage through to the actual removal of the image/content by the end-user or service provider.

3.10 Applying lessons learned from interviews to the victim-centred framework

As identified in Chapter 2, victims of IBSA have key needs which need to be addressed in order to be adequately remedied. Furthermore, Chapter 2 identified key

tools/mechanisms which can be used to address the needs of victims. These needs and tools/mechanisms are represented again in the table below.

Identified tools/mechanisms that address the needs of victims of IBSA

Identified needs of victims of IBSA	*Independent specialist authority*	*Individual complaints mechanism*	*Removal orders*	*Orders reducing visibility of IBSA material*	*Statutorily supported codes of practice*	*Educational campaigns*	*Civil avenues of redress*	*IBSA recognition as a criminal offence*
Constraining distribution of the image	+	+	+		+		+	+
Effective alternatives to constraining IBSA images	+	+		+				
Adequately trained and resourced authorities	+					+		
Prompt action	+	+	+	+	+			
Empowerment	+	+				+		+
Confidentiality	+	+						

Figure 11 Framework table illustrating the relationship between the needs of IBSA victims and the potential tools/mechanisms as informed by the Australian experience as developed in chapter 2

This table provides a framework to analyse to what extent the Australian approach to IBSA addresses victim needs. While Chapter 2 provided an introductory discussion of how the various Australian tools/mechanisms address victim needs, the interviews conducted in this chapter allows for an additional layer of insight when analysing the Australian context through a victim-centred lens. The following sections will go through each of the identified needs and consider to what extent the identified tools/mechanisms specific to the Australian context address these needs from the perspective of the stakeholders interviewed by the author. While the discussion of the needs in Chapter 2 identified each potential tool/mechanism that could address each need, this chapter will only discuss the tools/mechanisms addressed by interview candidates in relation to each need. Consequently, this discussion is supplemental to the discussion conducted in Chapter 2 whereby the general needs and tools/mechanisms were identified and subsequently applied to the Australian context. Considering the interviews from a victim-centred perspective and applying the developed framework allows the author to identify

any merits and potential pitfalls of the identified tools/mechanisms in addressing the needs of victim. The identification of these factors will assist in the analysis of the Irish situation in Chapter 4 and Chapter 5. Finally, the initial table displayed above in figure 10 will be refined through this analysis and outlined at the end of this section. This updated framework will then be used to provide a more nuanced victim-centred framework to be used in Chapter 4 and Chapter 5.

3.10.1 Constraining distribution of the image

In the context of the need for victims to constrain the distribution of their images, interview candidates highlighted some issues surrounding the tools/mechanisms of an independent statutory authority (OESC), an individual complaints mechanism (IBA portal), and removal orders (compliance notices).

As discussed in Chapter 2 the Enhancing Online Safety (Non-Consensual Sharing of Intimates Images) Act 2018 expanded the eSafety Commissioner's functions to include a complaints and objection system in relation to intimate images posted without consent known as the IBA Portal. Considering the removal of an intimate image is one of the 'most pressing priorities'[61] of victims, Section 32[62] and Section 33[63] of the Online Safety Act 2021, provide victims with a direct route to removal assistance through the IBA Portal. However, while the availability of such a mechanism is important, its ability to execute the function of removal assistance can face obstacles due to the challenges of the internet environment. As a result, it may not always be possible to fully address the need of victims to constrain the distribution of their images. This understanding was supported by insights gained from the interviews. For example, Bianca Fileborn explained that the OESC can only be effective to a certain point and that it is very hard to be sufficiently effective when it comes to removing harmful content online. She noted that it is very difficult for anyone, no matter how well-equipped, to remove an image permanently. One of the OESC's major barriers when removing harmful online content is the jurisdictional challenges that arise in the regulation of the internet.[64] 'Anonymous interviewee 1' confirmed that it is challenging for the OESC to meet the need of victims to constrain the

[61] Nicola Henry, Asher Flynn & Anastasia Powell, 'Policing Image-Based Sexual Abuse: Stakeholder Perspectives' (2018) 19 Police Practice and Research 577.
[62] As previously discussed, a person depicted in an intimate image, or an authorised person can make a complaint to the OESC through the IBA Portal under Section 32 of the Online Safety Act 2021.
[63] In addition, the IBA Portal allows for objection notices under Section 33 whereby a person can retract consent to an image and require a platform to no longer host their image. An objection notice may also be made in advance of an image being posted (i.e in response to a threat).
[64] See Chapter 1 section 1.2.4.

distribution of their images as some perpetrators may be located outside of Australia, and as a result, the OESC has no power to force these perpetrators to remove an intimate image. In addition, while an individual complaints mechanism can assist in the facilitation of removal with court assistance by means of a court order, Nicolas Suzor suggested that the IBA Portal should have greater legal power to take action initially without a court order. The ability of the IBA Portal to make a legal determination on what content should be removed would allow for images to be removed more quickly. This would address the need of victims to constrain the distribution of their image promptly and reduce the potential for widespread sharing.

The OESC can issue an array of removal orders known as 'compliance notices' to facilitate victims in the removal of their intimate image. As explained in Chapter 2 such notices include service provider notifications[65] (whereby the OESC can notify an online service provider that they are hosting an intimate image that was reported or objected to and to remove the image) or a removal notice[66] to an end user who posted an intimate image. Failure to comply with such notices can result in various enforcement actions including an injunction, enforceable undertaking, or a civil penalty by the OESC following a court order. Interviews supported the need for the OESC to have statutory power to issue removal orders and fines (civil penalties) in order to better remedy victims and be more effective in achieving its goals. 'OESC representative 1' highlighted that the mere ability to impose a sanction 'is what spurs people [intermediaries] on to remove content'.

3.10.2 Effective alternatives to constraining IBSA material

In the context of the identified need for effective alternatives to constraining IBSA material, the interviews expressed support for the mechanism/tool of orders reducing visibility of IBSA material (link deletion notices and app removal notices).

The provision of compliance notices provides the OESC with statutory powers to assist in the removal of intimate images therefore addressing victim's 'most pressing priorities'[67] and key 'desire'.[68] However as identified in the literature, removal of an

[65] Online Safety Act 2021, s 85.
[66] Online Safety Act 2021, s 77.
[67] Nicola Henry, Asher Flynn & Anastasia Powell, 'Policing Image-Based Sexual Abuse: Stakeholder Perspectives' (2018) 19 Police Practice and Research 577.
[68] Adrienne N. Kitchen, 'The Need to Criminalize Revenge Porn: How a Law Protecting Victims Can Avoid Running Afoul of the First Amendment' (2015) 90 Chicago-Kent Law Review.

intimate image from the internet following a removal order may not always be possible due to the potential for large scale instantaneous sharing and jurisdictional issues. This issue was confirmed in the interviews whereby 'OESC representative 1' acknowledged that in some cases the team struggles to remove the image. As a result, there is a need for alternative solutions to address the need of victims for removal. The provision of link deletion notices[69] and app removal notices[70] in the Online Safety Act 2021 empowering the OESC to direct a search engine provider or an app store to remove a link or app which provides access to reported harmful material particularly in cases where the content is hosted overseas, ensures reduced visibility of the intimate image. Referring to the voluntary precursor of the notices provided for in the Online Safety Act 2021, 'OESC representative 1' identified how these notices attempt to address victim's need for effective alternative solutions by at a minimum reducing the visibility of the content where removal is impossible.

3.10.3 Adequately trained and resourced authorities

As discussed in Chapter 2, a need to ensure that authorities are better able to provide support to IBSA victims has been identified. This will require such authorities to be adequately trained and resourced. The interviews conducted highlighted some issues in this area. Four participants suggested that the OESC required increased funding so to improve their technical capabilities. In particular the interviews identified the need for additional resources such as the provision of an additional avenue of communication for victims through a text messaging and an IT system that would support the timeframe recording of the removal processes from the initial reporting stage through to the actual removal of the image/content by the end-user or service provider. These resources are required to enable the OESC to adequately remedy victims.

Furthermore, the interviews identified that there is a lack of international collaboration for the removal of harmful content such as intimate images when hosted overseas. This is particularly an issue for content hosted on pornography sites hosted overseas. Interviews identified how law enforcement lack the resources to collaborate and work collectively to remedy victims of IBSA.

[69] Online Safety Act 2021, s 124.
[70] ibid s 128.

3.10.4 Prompt action

In the context of the identified need for prompt action, the interviews highlighted issues surrounding the tools/mechanisms of an individual complaints mechanism (IBA portal), removal orders (compliance notices), and civil avenues of redress.

A key need of IBSA victims is the provision of 'effective' responses. In the context of the IBA Portal, there is a need for increased technical support to more effectively provide redress. In particular, the IBA Portal needs to be equipped with the technical capabilities to record the time frame for image removal. This is vital considering victims require prompt removal so to minimise further distribution. 'OESC representative 1' and 'OESC representative 2' identified that the OESC has no way to monitor how long it takes to remove harmful content from when the initial report is made to when the content is removed. The current system they have is manual. As a result, it is challenging to identify whether the OESC removes content promptly.

The compliance notices available to the OESC must be adhered to within a 24-hour period. [71] The provision of a specified time frame addresses the need of victims for prompt action. However, where a notice is not complied with, the OESC must seek to impose a penalty which may take some time as a court order must be granted. As a result, Nicolas Suzor and Peter Clarke recommended that in order to effectively address the immediacy and scale of distribution in the online sphere, the OESC should be empowered to issue an injunction or a civil penalty following failed compliance with a notice without a court order, but which can later be appealed to a court. This would allow for faster action which may reduce the spread of the image leading to more effective redress.

The interviews identified that in practice the civil penalty regime is a slow process as in order to implement a fine or an injunction the OESC must seek a court order. Peter Clarke described the civil penalty regime as a 'very bureaucratic process' and as a result the process of bringing penalty regime proceedings is 'very slow and for that reason not effective'. Therefore, the image may already go viral by the time an order is sought from the court. As a result, Peter Clarke suggested the OESC needs to be equipped with 'preventive injunctive relief' whereby the OESC can issue an enforcement action requiring the image to be removed immediately and then reposted if no harm is found following an investigation and/or court appeal.

[71] Online Safety Act 2021, s 65, s 77, s 88, s 109, s 114.

3.10.5 Empowerment

In the context of the identified need for empowerment, the interviews discussed the tools/mechanisms of an independent specialist authority (OESC) and an individual complaints mechanism (IBA portal).

Nicola Henry noted the OESC plays a symbolic role as it takes responsibility away from victims and shows society that the Government is taking action and that perpetrators will be held accountable. The presence of such an authority empowers victims as it removes victim-blaming attitudes and creates an environment which encourages IBSA victims to report and seek justice.

Henry, Flynn, and Powell identify the enabling of victims to report IBSA and the provision of 'access to support' as an 'important measure'[72] which assists in empowering victims. The IBA Portal addresses this need by providing victims with a 'one-stop-shop'[73] to report IBSA. This was further confirmed in the interviews whereby Nicola Henry, Helen Campbell, and Nicolas Suzor highlighted the importance of the IBA portal as it acts as an 'alternative avenue of redress' providing victims with direct access to redress without the need to report to the police, notify a platform or engage in legal services.

However, in order for victims to be empowered they need to be aware of the OESC and the availability of the IBA portal. Unfortunately, four participants from the interviews expressed an opinion that there is a lack of awareness of the OESC and that it would benefit from increased visibility. Peter Clarke and Bianca Fileborn stated that they would not know about the body but for 'working in the field' of online regulation. 'Alannah & Madeline Foundation representative 2' and 'Alannah & Madeline Foundation representative 3' also experienced a low level of knowledge about the eSafety Commissioner in school settings suggesting that 'schools don't even know that they exist'. Consequently, while such an authority and reporting mechanism exist, it can only empower victims once they are aware they can avail of this avenue of redress.

3.10.6 Confidentiality

[72] Nicola Henry, Asher Flynn & Anastasia Powell, 'Policing Image-Based Sexual Abuse: Stakeholder Perspectives' (2018) 19 Police Practice and Research 577.
[73] Office of the eSafety Commissioner, 'Submission: Review of the Enhancing Online Safety Act 2015 and the Online Content Scheme' (2018) 120.

In the context of the identified need for anonymity, the interviews supported the mechanism of an individual complaints mechanism (IBA portal) in addressing this need. However, the interviews highlighted challenges surrounding the criminal justice process.

The IBA Portal provides a less invasive avenue of redress as victims do not need to have a public record of their report which would otherwise be made should the victim make a report to the police resulting in court action. Franks identified one of the most significant harms suffered by victims of IBSA as the 'unwanted subjection to public scrutiny'.[74] The IBA Portal allows victims to make their report outside of the public domain thus maintaining some element of confidentiality although not complete anonymity.

Similarly, to the desk-based research conducted in chapter 2, the interviews also confirmed that a criminal avenue of redress may not address victim's need for anonymity. Nicola Henry, Helen Campbell, and Nicolas Suzor explained that seeking assistance through the criminal justice system is not always the most suitable option for victims of sexual violence specifically. Victims are reluctant to go through the court process as they suffer re-traumatisation as their identity may be made public.

3.10.7 A refined victim-centred framework informed by interviews

Having conducted desk-based research into the Australian system and having considered that system further in light of the perspectives of key stakeholders, it is useful to include a table applying the victim-centred framework to the Australian system following the enactment of the Online Safety Act 2021. In line with this, the various cells in each of the columns representing the tools/mechanisms below identify the specific Australian implementation of each of these tools/mechanisms with reference to the law. The Australian implementation of the tool/mechanism is listed in a cell across from the identified need if it addresses that particular need to some extent.

[74] Mary Anne Franks, 'Unwilling Avatars: Idealism and Discrimination in Cyberspace' (2011) Columbia Journal of Gender and Law.

	Independent specialist authority	*Individual complaints mechanism*	*Removal orders*	*Orders reducing visibility of IBSA material*	*Statutorily supported codes of practice*	*Educational campaigns*	*Civil avenues of redress*	*IBSA recognition as a criminal offence*
Constraining distribution of the image	OESC - Online Safety Act 2021, s 26	IBA Portal - Online Safety Act 2021, Division 3	Compliance Notices: Service Provider Notifications -Online Safety Act 2021, s 85), Removal Notices - Online Safety Act 2021, s 77		Basic Online Safety Expectations Online Safety - Basic Online Safety Expectations) Determination 2022		Civil remedies, including damages and injunctive relief available	Criminal Code Act 1995 s 474.17(A)
Effective alternatives to constraining IBSA images	OESC - Online Safety Act 2021, s 26	IBA Portal - Online Safety Act 2021, Division 3		Link Deletion Notices – Online Safety Act 2021, s 124 and App Removal Notices - Online Safety Act 2021, s 128				
Adequately trained and resourced authorities	OESC - Online Safety Act 2021, s 26					'ThinkUKnow' campaign and 'Safe Sexting: No Such Thing' campaign		
Prompt action	OESC - Online Safety Act 2021, s 26	IBA Portal - Online Safety Act 2021, Division 3	Compliance Notices: Service Provider Notifications -Online Safety Act 2021, s 85), Removal Notices - Online Safety Act 2021, s 77	Link Deletion Notices – Online Safety Act 2021, s 124 and App Removal Notices - Online Safety Act 2021, s 128	Basic Online Safety Expectations Online Safety - Basic Online Safety Expectations) Determination 2022			
Empowerment	OESC - Online Safety Act 2021, s 26	IBA Portal - Online Safety Act 2021, Division 3				'ThinkUKnow' campaign and 'Safe Sexting: No Such Thing' campaign		Criminal Code Act 1995 s 474.17(A)
Confidentiality	OESC - Online Safety Act 2021, s 26	IBA Portal - Online Safety Act 2021, Division 3						

Figure 12 Refracted framework table of key needs and identified tools/mechanisms in the Australian context following the enactment of the Online Safety Act 2021

Following an application of the victim-centred framework to the Australian context, it can be shown that the innovative regulatory response to IBSA is quite successful in addressing the needs of victims of IBSA. The Australian response addresses each of the identified needs of victims, at least partially. Furthermore, the needs of victims are

addressed at times by more than one tool/mechanism. This provides victims with a choice which lends additional agency to the victim and their particular needs. For example, the identified need of 'constraining distribution of the image' can potentially be addressed by six out of the eight identified tools/mechanisms including by an independent statutory authority, an individual complaints mechanism, removal orders, statutorily supported codes of practice, civil avenues of redress, and the recognition of IBSA as a criminal offence. The application of the victim-centred framework highlights the importance of an independent specialist authority with extensive powers and the ability to respond to individual complaints as a significant achievement from a victim-centred perspective. Without the OESC many of the identified needs of victims would remain unaddressed. This is a key lesson to be drawn from the Australian system.

While the Australian approach has been assessed positively from a victim-centred perspective, it is not without limitation. By delving deeper into the desk-based analysis and interview findings, changes required in order to further improve the Australian response from a victim-centred perspective can be identified. The interviews, in particular, facilitated a deeper understanding of how the regulatory response functioned in practice. The more layered analysis allows for a more fine-grained assessment ensuring that the framework could be applied in a nuanced manner and not in a 'check-box' fashion. For example, a key insight from the interviews was that the Australian response would benefit from a more empowered regulator with the ability to make legal determinations without court intervention. While the OESC can issue a removal notice, this tool/mechanism can only be utilised following the granting of a court order. The process of obtaining such an order can be time consuming whereby in the meantime the image may rapidly spread across the internet. Another interesting finding that would not have been made without the interviews was that the Australian response would benefit from greater awareness for the OESC. While the OESC is a valuable tool/mechanism in the context of providing a victim-centred response, its lack of visibility to victims is disappointing and has implications for how well the system achieves its goals and addresses victim needs in practice. This insight informs the understanding in this thesis of the importance of a well-funded independent supervisory body with a significant public profile. A key lesson is that this requirement cannot be fully met by the establishment of a body that ostensibly fills these functions but lacks power, visibility, and a distinct identity. Overall, the establishment and expansion of the OESC over time is a significant achievement in providing victim-centred remedies and addressing the needs of victims in

the Australian context. Both the desk-based research and interviews largely confirmed the success of the body, while also enabling a more sophisticated understanding of what aspects of the OESC are essential to its success and what aspects could be further improved.

3.11 Conclusion

The research discussed in this chapter and Chapter 2 provide crucial insights into the effectiveness of the Australian response to IBSA from a victim-centred perspective. Based on the research discussed in Chapter 2 and Chapter 3, the OESC system has been found to be a positive development for the tackling of IBSA in Australia, although it is not without flaws. Some of these flaws have been resolved through changes brought about by the Online Safety Act while others remain unresolved. By discussing interviews with expert stakeholders with direct experience with the Australian regulatory system, this chapter provides insight into a system that had been operating to an extent sufficient to allow an informed assessment of its effectiveness. The lessons learned from this system provide valuable insight to assist in the development of a similar approach to online regulation in Ireland. Furthermore, understanding how the Australian system responded to identified issues through updated legislation provides another layer of context to be analysed and considered in the Irish context. The interviews conducted support the development of a regulatory system overseen by a statutory authority with enforcement powers.

The insights gained in this chapter and Chapter 2 help to inform the analysis of the Irish legislative and policy response in Chapter 4 and Chapter 5. Specifically, the refined victim-centred framework provides an important tool that is applied in Chapter 4 and Chapter 5 in order to facilitate a structured victim-centred analysis of the Irish context. As this thesis moves on to consider the Irish response to IBSA, the following statement from the Briggs Report on online safety regulation will be borne in mind: 'it should be recognised as a joint responsibility between industry, government and the community, with each having discrete roles to play.'[75]

[75] Lynelle Briggs, *Report of the Statutory Review of the Enhancing Online Safety Act 2015 and the Review of Schedules 5 and 7 to the Broadcasting Services Act 1992 (Online Content Scheme)* October 2018.

Chapter 4: Mapping the Development of the Irish Response to Image-Based Sexual Abuse from a Victim-Centred Perspective

4.1 Introduction

In Ireland, support for the criminalisation of image-based sexual abuse (IBSA) has been growing in recent years and has been widely supported since the publication of the Law Reform Commission (LRC) Report on Harmful Communications and Digital Safety in 2016. While legislative efforts were made in the interim, legislation criminalising IBSA was eventually enacted in late 2020 in the form of the Harassment, Harmful Communications and Related Offences Act. While the new targeted legislation is a positive tool for victims and potential victims of IBSA, the priority of many victims is to first regain control of their intimate image and later seek the prosecution of the perpetrator.[1] While the new legislation satisfies the second priority of victims, the primary sought after remedy remains a challenge in many cases. While the targeted legislation allows for the prosecution of certain IBSA crimes, gaps in remedies and enforcement persist.

As highlighted in Chapter 2 and Chapter 3, over a number of years Australia has introduced reporting schemes – including the IBA scheme, Cyberbullying Complaints Scheme, and Online Content Scheme – in an effort to tackle the challenge of harmful online content and to provide an avenue of redress for victims. From the research conducted in this thesis, the importance of the role of the Office of the eSafety Commissioner (OESC) and its associated structures is clear. Under the recently enacted Online Safety and Media Regulation Act 2022 (OSMRA), an Irish regulatory authority similar to the OESC called the Online Safety Commissioner (OSC) was established however it is yet to commence its functions and powers. Indeed, aspects of its role in relation to individual complaints and IBSA remain undecided and under review.

This chapter provides a detailed account of the Irish response to the issue of IBSA that has led to the point where an online safety body 'the OSC' has been established by the Irish government. Firstly, this chapter outlines key milestones which have influenced legislative and policy decisions related to IBSA in Ireland. From 2015 to 2020,

[1] Nicola Henry, Asher Flynn & Anatasia Powell, 'Policing IBSA: Stakeholders Perspectives' (2018) 19 Police Practice and Research 565.

legislative efforts concerning IBSA stalled, but numerous key events occurred during this time. These key milestones will be identified and discussed, showing how the current targeted legislation and proposals for enforcement responses were developed and formed. These discussions highlight Ireland's evolving approach to combating IBSA. Secondly, this chapter discusses the Harassment, Harmful Communications and Related Offences Act 2020 which criminalises IBSA in Ireland. The sections of the Act designed to target IBSA are discussed, and the merits and limitations of the legislation are identified. This chapter applies the victim-centred framework developed in Chapter 2 and refined in Chapter 3 in order to assess to what extent the Irish response to IBSA addressed the needs of victims prior to the development of the OSMRA.

Thirdly, this chapter provides important background to the OSMRA by mapping out its legislative development. This requires consideration of the general scheme of the Online Safety and Media Regulation Bill 2019 and the various submissions which informed its construction, the pre-legislative scrutiny of the general scheme of the bill, and the Online Safety and Media Regulation Bill 2022 (OSMRB). As a result, this chapter comprehensively maps out the Irish developments in the area of IBSA which have informed the development of the current Irish regulatory response. Mapping the Irish developments that led to the OSMRB and OSMRA assists with understanding the political context in which the legislation evolved. This provides useful insight when considering the role the concerns of victims played in the legislative process. There have been a number of incidents which have created political momentum for action in Ireland which will be discussed below. Within that context, the discussion of the Irish situation begins by highlighting the story of an Irish victim of IBSA.

4.2 Understanding the Irish context by identifying key milestones

The growing support for targeted legislation designed to tackle the issue of IBSA in Ireland is evident from the existence of several key reports, proposed legislation, Oireachtas debates, and national campaigns. Providing crucial impetus for these efforts was the increased recognition of the prevalence of and harm caused by IBSA. Cognisance of the harm grew in response to the reporting of numerous incidents of IBSA that illustrated the gaps in Irish law.

4.2.1 The case of 'Jane'

In one of the first academic articles concerning the issue of IBSA in Ireland, published in 2015, Walley highlighted that Ireland lacked 'specific statutory provisions to deal with 'revenge porn' and that the legislature may be 'obliged to follow other jurisdictions by fashioning dedicated cyber remedies'.[2] In 2016, the gap in protection received popular attention through the publication of the case of 'Jane' who shared her story pseudonymously with the Irish public.[3] Jane became a victim of IBSA when her ex-boyfriend uploaded an explicit video of them engaged in sexual intercourse which he covertly recorded. The video was accompanied with the writing '24-year-old female from Ireland who is pretty much up for anything'.[4] 'Jane' reported her case to the Gardaí however they were unable to provide an adequate response.[5] The Gardaí informed Jane that there was 'nothing' they could do due to the lack of legislation.[6] This case demonstrated how victims lacked support from the authorities in Ireland and that the avenues for redress were uncertain.[7] The Gardaí lacked the power to pursue the distributors of IBSA and remained unsure as to their authority in such cases.[8] The publication and discussion of Jane's story represented a significant turning point in the Irish public discourse on IBSA that clearly highlighted the need for targeted legislation.

4.2.2 The Law Reform Commission's Report on Harmful Communications and Digital Safety

On the 27th of September 2016, the LRC released a report which included recommendations for new legislation dealing with harmful communications and digital safety.[9] The report included a draft Harmful Communications and Digital Safety Bill, which was proposed as a model for implementation, and a report from two workshops conducted with 70 people aged between 13–17 years. The LRC report outlined the laws that applied to harmful communications – including IBSA – in Ireland at the time and

[2] Pauline Walley, 'In Memory Amore: Revenge, Sex and Cyberspace' (2015) 20(2) The Bar Review 33.
[3] Claire McCormack, 'Revenge Porn Nightmare: 'I felt I was Completely Violated'' *Irish Independent* (Dublin, 12 June 2016).
[4] ibid.
[5] ibid.
[6] Vadim Geiorgiev, 'It Made Me Feel Really Dirty' - Victim Powerless Against Revenge Porn Attack' *The Journal* (21 June 2016).
[7] Daire Courtney, 'There was Nothing the Guards Could Do For Me' - Victim of Revenge Porn Speaks Out' *Irish Independent* (Dublin, 27 September 2016).
[8] Conor Lally, 'Gardaí have 'limited scope' on 'revenge porn'' *Irish Independent* (Dublin, 22 April 2015).
[9] Law Reform Commission, *Harmful Communications and Digital Safety* (LRC 116 — 2016).

recommended reform. The LRC highlighted how the law had failed to react to developments in technology and as a result failed to sufficiently protect victims of online crimes in Ireland.[10] At the time, the then Minister for Justice Frances Fitzgerald supported the drafting of a Bill to provide for new offences – including an IBSA offence – and to extend existing criminal offences in order to address gaps in the law brought about by changes in society and technology. Fitzgerald noted that the speed and scale of modern communication can magnify the damage done to victims and as such 'it is important that our laws can deal effectively with these issues'.[11] The LRC proposal of a consolidated piece of legislation consisting of existing criminal laws in the area of harmful communications together with proposals designed to deal with new forms of harmful communications offered notable advantages over a piecemeal approach. The LRC report also proposed the establishment of a Digital Safety Commissioner (DSC) to enforce the removal of online harmful content.[12] The report provided Ireland with the first detailed proposal on how to combat IBSA and informed the current targeted legislation enacted under the Harassment, Harmful Communications and Related Offences Act 2020. Considering the impact the LRC report and model legislation had on the actual legislation, it is important to analyse the proposals in greater detail.

4.2.2.1 The Law Reform Commission's model legislation for image-based sexual abuse

Two sections of the LRC model legislation – Sections 4 and 5 – were designed to outlaw IBSA. Section 4 of the LRC model states:

> 4. (1) A person commits an offence where he or she, without lawful authority or reasonable excuse and in the circumstances referred to in subsection (2), by any means of communication distributes or publishes an intimate image of another person (in this section referred to as the other person) without the consent of the other person, or threatens to do so.
> (2) The circumstances are that the person who distributes or publishes the intimate material, or who threatens to do so, does so where—
> (a) he or she, by his or her act or acts intentionally or recklessly seriously interferes with the other person's peace and privacy or causes alarm, distress or harm to the other person, and

[10] ibid para 2.
[11] RTE News, 'Revenge Porn, Cyber Stalking to become illegal offences' < https://www.rte.ie/news/2016/1231/841957-revenge-porn-cyberstalking-bill/ > accessed 17 May 2017.
[12] Draft Harmful Communications and Digital Safety Bill 2016, s 18(2).

> (b) his or her act or acts is or are such that a reasonable person would realise that the actor acts would seriously interfere with the other person's peace and privacy or cause alarm, distress or harm to the other person.[13]

This section was designed to address cases involving the disclosure of intimate images without consent with the intent to cause harm or with recklessness as to the resulting harm caused. The LRC described these acts as very 'serious behaviour'[14] and stated that this section represents 'typical' cases of IBSA.[15] The LRC also highlighted that this section also accounts for threats to disseminate the victim's intimate image. It clarified that a 'once off' distribution of an intimate image is sufficient to amount to an offence under this proposed section.[16] Under the LRC model legislation, if convicted summarily, a perpetrator could be subject to a class A fine or imprisonment for a term not exceeding 12 months or both. If convicted on indictment, a perpetrator could be subject to a fine or imprisonment for a term not exceeding 7 years or both.

The LRC model legislation also included an additional offence in Section 5:

> 5. (1) A person commits an offence where he or she, without lawful authority or reasonable excuse and in the circumstances referred to in subsection (2), by any means of communication takes, or distributes or publishes an intimate image of another person (in this section referred to as the other person) without the consent of the other person.
> (2) The circumstances are that the person who takes, or distributes or publishes the intimate material does so where he or she, by his or her acts seriously interferes with the other person's peace and privacy or causes alarm, distress or harm to the other person.[17]

The LRC recognised that in some cases content is shared spontaneously or without considering the impact on the victim, especially when young people are involved.[18] The LRC explained that these cases do not have intent to cause harm. It justified the requirement for a separate section to govern cases whereby the accused acted 'neither intentionally or recklessly' but rather the crime was committed 'simply by taking, distributing or publishing' an intimate image without consent.[19] Under the LRC model

[13] ibid s 4.
[14] Law Reform Commission, *Harmful Communications and Digital Safety* (LRC 116 — 2016) para 2.
[15] ibid.
[16] ibid.
[17] Draft Harmful Communication and Digital Safety Bill 2016, s 5.
[18] Law Reform Commission, *Harmful Communications and Digital Safety* (LRC 116 — 2016) 193.
[19] Law Reform Commission, *Harmful Communications and Digital Safety* (LRC 116 — 2016) 193.

legislation, summary conviction under Section 5 could result in a class A fine or imprisonment for a term not exceeding 6 months or both.[20] This section does not provide for an indictable offence.

Two issues not adequately addressed by the LRC Report or by Sections 4 and 5 of the LRC model legislation, are whether the commercialisation of IBSA should be considered an explicit aggravated factor when sentencing and whether an act of IBSA should be considered 'less serious' solely on the matter of lack of intent. The commercialisation of IBSA should be considered to be an aggravating factor when contemplating a sentence or calculating a fine. It should be noted that the intent to extort money or gain financially is a common reason to commit IBSA. This is evident through the multiple 'revenge pornography' websites which have been set up for commercial gain through the extortion of money as outlined in Chapter 1. Examples of these are Hunter Moore's website 'IsAnyoneUp.com' and Kevin Bollaert's website 'UGotPosted.com'. In both of these cases the individuals who hosted the websites and thus distributed the material to a wide audience did not know the victims. Whether or not these website hosts intended to cause harm to their victims, it certainly seems that they were reckless as to the potential for harm to be caused. Explicitly including financial gain as an aggravating factor should disincentivise the harmful practice. Crucially, however, the absence of intent to make a financial gain should not prevent judges from applying the maximum penalty allowed where the victim has been substantially harmed by the distribution of their image without consent.

Secondly, the question of what makes an act of IBSA 'less serious' must be discussed. According to the LRC report, the proposed Section 5, as set out by the LRC in the model legislation, is proposed to deal with 'less serious' offences of IBSA.[21] The Commission stated that the intention was that this section would apply to 'less serious'[22] offences, i.e. where such offences 'fall short of being intentional or egregious'.[23] Section 5 was proposed as a strict liability offence therefore the requirement of intent or negligence is not necessary. The LRC report also pointed out that this proposed section would apply only to images taken without consent. Examples of potentially 'less serious' offences identified as governable by the proposed Section 5 included what is colloquially known as 'up-skirting' and 'down-blousing' where they are committed without intent or

[20] ibid.
[21] ibid 194.
[22] ibid.
[23] ibid.

recklessness to cause harm.[24] Under the LRC model legislation, summary conviction under Section 5 could result in a class A fine or imprisonment for a term not exceeding 6 months or both.[25] Section 5 did not provide for an indictable offence.

The LRC discussion of the model law appears to determine the seriousness of an act of IBSA solely on the lack of intent. While the 'less serious' designation is not mentioned in Section 5 of the LRC model legislation itself, its use to describe Section 5 offences in the LRC report and the explanatory note under Section 5 is potentially significant. While intent or recklessness are factors to be considered when deciding on whether a crime is less serious, the equating of the intent question with particular forms of IBSA – notably 'up-skirting' and 'down-blousing' – in the report and discussion of the model legislation seems questionable. Potentially part of the reasoning rests on the idea that the identifiability of the victim affects the seriousness of an offence of IBSA.[26] The greater the identifiability of the victim in the image, the greater the potential harm to the victim and thus greater the intent to cause harm.[27] Identifying factors can take many forms which do not relate solely to the subject's facial features. Identifiers can include objects in the background, for example, a picture on the wall behind the victim, a certificate with a name in the image or a particular setting like a college apartment. Identifiers can also include specific marks on the subject captured in the image – such as distinctive tattoos, piercings or birth marks.[28] Moreover, individuals can of course be identified through the use of labels or tags on an image that connect the image with information such as names or nicknames, addresses, email addresses, employment, and personal contact numbers. In such circumstances, the harm to the victim remains.

Another issue worth considering in the LRC model legislation is the choice of definitions. The LRC model legislation defines an intimate image as:

> "intimate image" means a visual recording of a person made by any means including a photographic, film or video recording (whether or not the image of the person has been altered in any way)—
> (a)(i) of the person's genital or anal region or in the case of a female of her breasts (whether the genital or anal region or, as the case may be, the breasts are covered by underwear or are bare), or

[24] Sarah Bardon, 'Upskirting', Cyberstalking, and Revenge Porn to be Criminal Offences' *Irish Times* (Dublin, 15 May 2017).
[25] Draft Harmful Communication and Digital Safety Bill 2016, s 5.
[26] Scott Stroud, 'The Dark Side of the Online Self: A Pragmatist Critique of the Growing Plague of Revenge Porn' (2014) 29 Journal of Mass Media Ethics 168.
[27] ibid.
[28] ibid.

(ii) in which the person is nude, is exposing his or her genital organs or anal region or in the case of a female is exposing her breasts, or
(iii) in which the person is engaged in explicit sexual activity,
and
(b) in respect of which, at the time of the recording, there were circumstances that gave rise to a reasonable expectation of privacy (and such circumstances can include that the recording was made when the person whose image was recorded was in a public place),
and
(c) in respect of which the person depicted retains a reasonable expectation of privacy at the time the image is communicated.[29]

This definition aims to capture images that depict all types of nudity, sexual activity, and private areas covered by underwear. Unfortunately, this definition does not define underwear or expand on what is regarded as underwear. As a result, this definition does not include or consider provocative clothing. What if the person in the image is fully clothed or is wearing an ensemble of a suggestive or 'kink' related nature? For example, certain items of clothing may not be what a person would choose to wear in public yet may not be categorised as underwear or expose any of the body parts outlined in the proposed definition. It would appear that an image capturing a person posing in such clothing would not be considered 'intimate' under this definition, yet if this image was posted online without consent the harm could be equivalent regardless of the lack of nudity or sexual activity. The struggle with this definition highlights that rigid definitions may not adequately protect those affected. However, the fact that an 'intimate image' is defined to include an image 'whether or not the image of the person has been altered in any way' suggests that the LRC model legislation intends the definition to include images which have been 'photo-shopped'. This would appear to imply that images that have been altered technologically by transposing a person's face onto a sexually explicit body are included by the model legislation definition. This would appear to capture the harms caused by photoshopping and the more technologically sophisticated practice of generating 'deep fakes'.[30]

[29] Draft Harmful Communication and Digital Safety Bill 2016, s 2.
[30] Asher Flynn, Anastasia Powell, Adrin Scott, & Elena Cama, 'Deepfakes and Digitally Altered Imagery Abuse: A Cross-Country Exploration of an Emerging form of Image-Based Sexual Abuse' (2021) British Journal of Criminology; Dean Fido, Jaya Rao & Craig A.Harper, 'Celebrity Status, Sex, and Variation in Psychopathy Predicts Judgements of and Proclivity to Generate and Distribute Deepfake Pornography' (2022) 129 Computers in Human Behaviour; Russell Spivak, '"Deepfakes": The Newest Way to Commit one of the Oldest Crimes' (2019) 3 Georgetown Law Technology Review 339; Douglas Harris, 'Deepfakes: False Pornography is here and the Law Cannot Protect You' (2018) 17 Duke Law and Technology Review 99.

In spite of the points raised in this section, the proposed offences contained in the LRC model legislation provided a good starting point for how the Oireachtas could legislate for a targeted IBSA law. Aside from recommending the creation of these offence, the other significant contribution of the LRC report was the recommendation for the establishment of a Digital Safety Commissioner.

4.2.2.2 The Law Reform Commission's proposed Digital Safety Commissioner

In 2016, the LRC conducted two consultative workshops with 70 people aged between 13–17 years facilitated by the Department of Children and Youth Affairs. This consultation involved two sessions on the 27th and 28th of April 2016, with 36 young people attending on the first day and 34 young people attending on the second day. An independent report of the consultations was prepared.[31] Results from this study highlighted that young people struggle to remove content from the internet.[32] The young people who engaged in the workshops argued for greater social media intervention, recommending 'that all social media websites should make it easier to report and take down content from the internet'[33] As a result, the LRC highlighted the need for an oversight system to promote digital safety, including an efficient take down procedure for harmful digital communications.[34] In Part 3 of the LRC model legislation, the LRC proposed the establishment of a statutory Digital Safety Commissioner,[35] modelled on Australia's OESC.

The proposed DSC's purpose was to support and provide digital safety measures and act as an educational body to promote positive digital citizenship among children and young people. It would perform functions including the promotion of digital safety, implementation of measures to improve digital safety, provide effective takedown procedures, ensure the takedown procedures are available and easily accessible to all victims free of charge, produce guidance materials for online digital safety, collaborate with other government bodies and organisations on online safety, support and conduct research about digital safety, and publish papers and reports.[36] With regard to the takedown procedures, under the LRC proposed statutory system, individuals would

[31] Law Reform Commission, *Harmful Communications and Digital Safety* (LRC 116 — 2016) Appendix B.
[32] ibid.
[33] ibid.
[34] ibid para 44.
[35] Draft Harmful Communications and Digital Safety Bill 2016, s 18(2).
[36] ibid s 19.

initially apply directly to a social media site to request the removal of their intimate image in accordance with agreed time periods. If a social media site did not comply with the standards in the Code of Practice, the individual could then appeal to the DSC, who could direct a social media site to comply with the standards in the Code. If a social media site did not comply with the DSC's direction, the Commissioner could apply to the Circuit Court for a court order requiring compliance. This proposed system aimed to provide victims with a definite course of action. It also supplied a procedure which was better focused on remedying the victim.

The LRC report on Harmful Communications and Digital Safety highlighted Ireland's lack of protection against IBSA. The necessity of a dual approach of both criminalising the act of IBSA and placing greater responsibility and obligations on service providers to facilitate the removal of intimate images was clear. The report demonstrated the importance of removing harmful online content and implementing a clear and accessible process for victims of harmful communications, including victims of IBSA. While it is difficult to assess the efficacy of social media companies' content and conduct policies and reporting and removal procedures,[37] the LRC consultation with young people identified challenges with the removal of online content suggesting that the self-regulation of intermediaries and social media platforms is ineffective.

4.2.3 The case of Dara Quigley

In 2017, the prevalence of IBSA and the lack of accountability for those who carry out this abuse was a renewed topic of media attention following a tragic event.[38] On the 12th of April 2017, journalist and online blogger Dara Quigley took her own life five days after an intimate video was posted online and viewed more than 100,000 times.[39] In 2017, members of An Garda Síochána detained Ms Quigley under Ireland's Mental Health Act

[37] Sandra Laville, 'Top Tech Firms Urged to Step Up Online Abuse Fightback' *The Guardian* (11 April 2016).

[38] Connor Feehan, 'Garda who Filmed Tragic Journalist Dara Quigley to Avoid Prosecution' *The Irish Independent* (Dublin, 4 August 2018); Kitty Holland, 'Dara Quigley's Family 'Battling State' to Find Out Key Events Before Death' *Irish Times* (Dublin, 23 October 2019); Shauna Bowers, 'Government Urged to Outlaw Creation and Sharing of Private Sexual Images' *The Irish Times* (Dublin, 8 October 2019); Connor Gallagher, 'Family of Dara Quigley Yet to be Contacted by Garda Management' *The Irish Times* (Dublin, 8 August 2018); Connor Gallagher, 'Garda who Shared Video of Mentally Ill Woman Will Not Face Charges' *The Irish Times* (Dublin, 7 August 2018); Sarah Burns, 'Dara Quigley Case: Inquiry Under Way into Possible Data Breach' *The Irish Times*, Dublin, 14 May 2017); Marie O'Halloran, 'Tánaiste 'Appalled' at CCTV Footage of Dara Quigley Appearing Online' *The Irish Times* (Dublin, 11 May 2017).

[39] Marie O'Halloran, 'Tánaiste 'Appalled' at CCTV Footage of Dara Quigley Appearing Online' *The Irish Times* (Dublin, 11 May 2017).

for walking naked on a Dublin street.[40] The CCTV footage of her walking naked and being detained was kept by the Gardaí.[41] A member of the An Garda Síochána recorded the CCTV footage and disseminated the intimate material on WhatsApp. The material was subsequently shared on Facebook and in total was shared over 125,000 times.[42] The Garda accused of sharing the footage did not face criminal charges due to the lack of targeted legislation criminalising the sharing of intimate images without consent and instead underwent an internal investigation by the Garda Síochána Ombudsman Commission.[43] Many organisations such as the Dublin Rape Crisis Centre and the Irish Council for Civil Liberties called for the criminalisation of IBSA as a result of this case providing further impetus to the demand for legislative action.[44]

4.2.4 The Harassment, Harmful Communications and Related Offences Bill 2017

In May 2017, the Labour Party TD, Brendan Howlin, published a Private Member's Bill with the title, Harassment, Harmful Communications and Related Offences Bill 2017. If enacted, this Bill would have criminalised IBSA in line with the LRC recommendations.[45] Section 4 of the Private Member's Bill intended to criminalise the distribution of intimate image without consent and threats to distribute intimate images.[46] While the Bill follows

[40] Rónán Duffy, 'Deplorable and Revolting' Treatment of Deceased Activist Dara Quigley is Raised in the Dáil, (*The Journal*, 11 May 2017) < https://www.thejournal.ie/dara-quigley-dail-3384651-May2017/ > accessed 22 February 2022.

[41] Conor Gallagher, 'Garda who Shared Video of Mentally Ill Woman Will Not Face Charges' *The Irish Times* (Dublin, 7 August 2018)

[42] Rónán Duffy, 'Deplorable and Revolting' Treatment of Deceased Activist Dara Quigley is Raised in the Dáil, (*The Journal*, 11 May 2017) < https://www.thejournal.ie/dara-quigley-dail-3384651-May2017/ > accessed 22 February 2022; Sarah Burns, 'Dara Quigley Case: Inquiry Under Way into Possible Data Breach' *The Irish Times* (Dublin, 14 May 2017)

[43] Connor Feehan, 'Garda who Filmed Tragic Journalist Dara Quigley to Avoid Prosecution' *The Irish Independent* (Dublin, 4 August 2018).

[44] The Irish Council for Civil Liberties, 'ICCL Brings Dara Quigley Case to Justice Committee' (22 October 2018) < https://www.iccl.ie/news/dara-quigley-justice-committee/ > accessed 16th June 202; Elizabeth Farries, Doireann Ansbro, & Grace Tierney, 'The Irish Council for Civil Liberties Online Harassment Submission' to the Joint Committee on Justice and Equality (6th October 2019).

[45]Ciarán D'Arcy, 'Labour Publishes Bill to Criminalise Revenge Porn' *Irish Times* (Dublin, 4 April 2017).

[46]Harassment, Harmful Communications and Related Offences Bill 2017, Section 4 states: Distributing, etc., intimate image without consent 4. (1) A person who without lawful authority or reasonable excuse— (a) records, distributes or publishes, or threatens to record, distribute or publish, an intimate image of another person without the other person's consent, and (b) by those acts seriously interferes with the peace and privacy of the other person or causes alarm, distress or harm to the other person, is guilty of an offence and is liable— (i) on summary conviction to a Class A fine or to imprisonment for a term not exceeding 6 months or to both, (ii) where the offence was committed intentionally or recklessly and a reasonable person would have realised that those acts would seriously interfere with the other person's peace and privacy or cause alarm, distress or harm to the other person— (I) on summary conviction to a Class A fine or to imprisonment for a term not exceeding 12 months or to both, or (II) on conviction on indictment to a fine or to imprisonment for a term not exceeding 7 years or to both;

key recommendations made by the LRC Report, it did not provide for a DSC. Brendan Howlin's reasoning for this was that 'creating a new statutory agency is outside the remit of a Dáil Private Member's Bill'.[47] The Bill passed the second stage in the Dáil without opposition and as of the 31st of January 2018 the Bill was before the Dáil third stage where the Bill was examined section by section. The then Minster for Justice Charlie Flanagan noted that the Bill was 'broadly similar to legislation being drafted within my own department at present, though I appreciate that process is taking longer than I would have wished'.[48] While Flanagan stated that he was 'entirely in support of the intention and spirit behind the Deputy's Private Member's Bill' he maintained that a 'significant number of amendments would be required' before the Bill could be safely enacted.[49] In May 2019, the Government confirmed its acceptance of Labour's Private Member's Bill and decided to stop working on its own similar Bill. However, on the 14th of January 2020 the Harassment, Harmful Communications and Related Offences Bill lapsed following the dissolution of the Dáil and Seanad. However, the 'Discord Leak' outlined in due course in section 4.2.9 prompted the un-shelving of this legislation in October 2020.

4.2.5 The Digital Safety Commissioner Bill 2017

In November 2017, Sinn Féin TD, Donnchadh Ó Laoghaire sponsored the Private Member's Bill entitled, the Digital Safety Commissioner Bill 2017. The Bill was referred to the Committee Stage of the Dáil on the 22nd of February 2018 and subsequently did not progress. In spite of this, the contents of the Bill are worth considering. The key function of the proposed legislation was to 'establish an office of a Digital Safety Commissioner and to provide for its functions to ensure oversight and regulation of procedures for removal of harmful digital communications, to provide for the creation of codes of practice for digital service undertakings, to establish an advisory committee to the Digital Safety Commissioner, and to provide for related matters'.[50] Overall this Bill followed the recommendations of the Law Reform Commission's report on Harmful Communications and Digital Safety; however, one of the significant differences was the

[47] Labour Admin, 'Howlin speech at launch of Harassment, Harmful Communications and Related Offences Bill 2017' < https://labour.ie/news/2017/04/04/howlin-speech-at-launch-of-harassment-harmful-communications-and-related-offences-bill-2017/ > accessed 24 January 2022.
[48] Department of Justice, 'Private Member's Bill - Harassment, Harmful Communications and Related Offences Bill 2017' (9 August 2021) < https://www.gov.ie/en/speech/a85138-private-members-bill-harassment-harmful-communications-and-related-o/ > accessed 24 January 2022.
[49] ibid.
[50] Digital Safety Commissioner Bill 2017.

establishment of an advisory committee. The Advisory Committee, as proposed under the Private Member's Bill would be focused on the wider community with 50% of its members drawn from civil society organisations, 25% from industry groups and, 25% from relevant Governmental departments or statutory bodies.[51] Young people were also proposed to sit on this committee.[52] The purpose of this committee was to ensure that new developments, technologies, trends, and platforms would be brought to the attention of the Commissioner as quickly as possible ensuring that the Office has the ability to evolve with technology.[53] The Bill lapsed on the 14th of January 2020 following the dissolution of the Dáil and Seanad. However, the discussions and debates at the time around this proposed Bill informed the drafting of later legislation and proposals for the Government's current enforcement response to IBSA. As a result, these discussions are analysed next.

Overall, the Bill was welcomed by society in general and by many youth focused organisations, including the Irish Society for the Prevention of Cruelty to Children, the Ombudsman for Children, and CyberSafe Ireland. [54] A report from the Oireachtas Committee on Children and Youth Affairs found that the establishment of a Digital Safety Commissioner was a 'necessity'.[55] While the then Minister for Communications, Climate Action and Environment, Denis Naughton had broadly supported the concept of a DSC, the then Taoiseach, Leo Varadkar, was not 'so enthusiastic in his support'.[56] The then Taoiseach told the Dáil he was not opposed to the idea but acknowledged that 'policing the internet has its difficulties'.[57] Minister Naughton highlighted certain concerns which he felt must be addressed before such a body could be implemented. Such concerns included jurisdictional issues, definitional issues, clarity as to what role the courts have where an entity is established outside of the State and clarity as to the obligations imposed by the Bill on digital service undertakings.[58] This highlighted how a general consensus was still to be reached as to how such challenges could be resolved.

[51] ibid s 11(4).
[52] ibid s 11(5).
[53] ibid s 11(1).
[54] Tim O'Brien, 'Cyberbullying Watchdog Office Should Open Without Delay' *Irish Times* (Dublin, 29 March 2018).
[55] Houses of the Oireachtas, Joint Committee on Children and Youth Affairs, *Report on Cyber Security for Children and Young Adults* (32 CYA 011 — March 2018).
[56] Dáil Eireann Debate, 'Digital Safety Commissioner Bill 2017: Second Stage [Private Members]' (22 February 2018) < https://www.oireachtas.ie/en/debates/debate/dail/2018-02-22/30/#s33 > accessed 27 August 2018.
[57] ibid.
[58] ibid.

Member of the opposition party Fianna Fáil,[59] Deputy Ann Rabbitte, extended support for the Digital Safety Commissioner Bill and criticised the lack of legislative action by the Government. She criticised the then Taoiseach for calling on technology companies to take greater responsibility and do more to protect people from online dangers. Criticising this apparent endorsement of self-regulation from the then Taoiseach, Deputy Rabbitte argued that the Government had effectively 'washed its hands of any obligation to protect citizens from the online world'.[60] Members of the opposition and Labour party, Deputy Seán Sherlock expressed support for the Bill but suggested that there was a lack of assertions of 'ownership' of a DSC Office by Governmental departments stating 'not one of them is proactive in putting up his or her hand and asking for responsibility for the role of a Digital Safety Commissioner within his or her Department'.[61]

On the 29th of March 2018, the Joint Committee on Children and Youth Affairs Report on Cyber Security for Children and Young Adults was released and made eighteen recommendations for the enhancement of online safety for children and young adults. The report expressed strong support for the establishment of a DSC. The report described its implementation as a 'necessity'.[62] The report was informed by experts in online child safety most notably Dr. Geoffrey Shannon,[63] Professor Brian O'Neill,[64] Professor Barry O'Sullivan,[65] and Dr. Mary Aiken.[66] Engagement with these experts confirmed the need for a DSC similar to the proposal set out by the LRC. The report did recommend certain amendments, however. These included a recommendation that the proposed DSC should be required to take down harmful material within a 'specified period of time'[67] and the DSC should receive direction from an 'advisory group'.[68] Following this report, public and media support for the implementation of a DSC was expressed.[69] While support was

[59] Fianna Fáil were in a 'confidence and supply' arrangement with the Government at the time.
[60] Dáil Eireann Debate, 'Digital Safety Commissioner Bill 2017: Second Stage [Private Members]' (22 February 2018) < https://www.oireachtas.ie/en/debates/debate/dail/2018-02-22/30/#s33 > accessed 27 August 2018.
[61] ibid.
[62] Houses of the Oireachtas, Joint Committee on Children and Youth Affairs, *Report on Cyber Security for Children and Young Adults* (32 CYA 011 — March 2018) 18.
[63] Special Rapporteur on Child Protection.
[64] CyberSafe Ireland.
[65] School of Computer Science & IT at University College Cork.
[66] Professor of Cyberpsychology and Chair of the Department of Cyberpsychology at Capitol Technology University, Washington.
[67] Houses of the Oireachtas, Joint Committee on Children and Youth Affairs, *Report on Cyber Security for Children and Young Adults* (32 CYA 011 — March 2018)19.
[68] ibid.
[69] Tim O'Brien, 'Cyberbullying Watchdog Office Should Open Without Delay' *Irish Times* (Dublin, 29 March 2018).

expressed for the DSC implementation by many, criticism was extended by industry representatives who argued that the obligations would be onerous for providers.[70]

Overall, these discussions highlighted the need for an oversight body with statutory powers designed to help tackle online harms, including to provide for the removal of harmful digital content such as intimate images.

4.2.6 The Open Policy Debate on Online Safety

Another key milestone which also demonstrates challenges evident in the regulation of IBSA in Ireland is the Open Policy Debate on Online Safety held on the 6th of March 2018. The Government acknowledged that a number of initiatives, reports, and recommendations with regard to online safety had influenced their response to online crime however further open policy debate was still required to help inform how Ireland should progress in this complex matter with input from all key stakeholders.[71] The Open Policy Debate was organised by the then Minister for Communications, Climate Action and Environment, Denis Naughten with the support of five other Government Departments including Justice & Equality; Education & Skills; Business, Enterprise and Innovation; Health; and Children and Youth Affairs.[72] More than '100 delegates and speakers' working across 'industry, non-profit organizations, government and the EU' attended and participated at the event. The overall aim was to raise awareness among all participants of the work and activities being undertaken by Government, the European Commission, industry and NGOs in the area of digital safety while also identifying any 'gaps and opportunities for closer co-operation'[73] The debate highlighted challenges facing Ireland with regard to online safety in general but also the removal of harmful content such as intimate images. Firstly, the then Taoiseach Leo Varadkar revealed that policymakers were unsure as to the appropriate role for Government in responding to online risks such as IBSA.[74] Varadkar spoke about the risks on the internet and how a key

[70] Elaine Loughlin, 'ISPCC: Child Safety Measures Don't Go Far Enough' *Irish Examiner* (Dublin, 30 March 2018).
[71] Department of Communications, Climate Action and Environment, 'Open Policy Debate Online Safety' (Royal Hospital Kilmainham, 6 March 2018).
[72] Irish Government News Service, 'Naughten hosts Government's Open Policy Debate on Digital Safety' < https://merrionstreet.ie/en/news-room/releases/naughten_hosts_government%E2%80%99s_open_policy_debate_on_digital_safety.html> accessed 24 January 2022.
[73] ibid.
[74] Department of Communications, Climate Action and Environment, 'Open Policy Debate Online Safety' (Royal Hospital Kilmainham, 6 March 2018) 3.

aspect of the Open Policy Debate was to discuss 'the Government's role in responding to those risks'.[75] Detective Superintendent Declan Daly, representative from An Garda Síochána, highlighted current dangers online and specifically mentioned 'sexmailing' where information or images are used to blackmail people, 'harvesting' where settings are left open or unsecured allowing perpetrators to take images and use them, and 'sexting' which is the sharing of self-generated images.[76] All of these particular dangers raised by the Detective Superintendent Daly are directly related to IBSA highlighting its prominence as a problem in Ireland. Many representatives from organisations including the Children's Rights Alliance questioned whether the Gardaí have the powers and resources required to combat illegal content.[77]

Research from other jurisdictions shows policing limitations in cases of IBSA. In a survey of 783 police agents in the UK, Bond and Tyrrell found that respondents had a limited understanding of IBSA and a lack of confidence in investigating and responding effectively to victims.[78] Bond and Tyrrell found almost 95% of police 'had not received any formal training on how to conduct investigations into revenge pornography'. [79] In an Australian study, Henry and Powell identified police training as crucial to addressing IBSA. One participant to their qualitative study stated 'there needs to be a lot more on-going training . . . about the nature and dynamics of domestic violence and, specifically, including technology-facilitated stalking and abuse broadly, including non-consensual sharing of intimate images'.[80] At the Open Policy Debate the ISPCC noted a report of the Garda Inspectorate which stated that the Gardaí do not have sufficient resources to deal with issues related to harmful online content.[81]

During the session there was an opportunity for stakeholder participation. The participants were divided into 15 tables with a facilitator at each table to chair the discussion, ensuring all participants had an opportunity to contribute, and finally reporting back to the wider audience. The participants included representatives from many stakeholder groups including Google, Facebook, the Press Council of Ireland, Sky Ireland, the Broadcasting Authority of Ireland, Dublin Institute of Technology, Rape

[75] ibid.
[76] ibid 8.
[77] ibid.
[78] Emma Bond & Katie Tyrrell, 'Understanding Revenge Pornography: A National Survey of Police Officers and Staff in England and Wales' (2021) 36 Journal of Interpersonal Violence 2166.
[79] ibid.
[80] Nicola Henry, Asher Flynn & Anastasia Powell, 'Policing Image-Based Sexual Abuse: Stakeholder Perspectives' (2018) 19 Police Practice and Research, 565.
[81]Department of Communications, Climate Action and Environment, 'Open Policy Debate Online Safety' (Royal Hospital Kilmainham, 6 March 2018) 15.

Crisis Network Ireland, Dublin College University, the National Anti-Bullying Centre, CyberSafe Ireland, the Department of Education and Skills, the HSE, the National Office for Suicide Prevention, the Irish Society for the Prevention of Cruelty to Children, and the Department of Children and Youth Affairs.[82] The report did not identify which participants made a particular argument or point but rather represented the arguments made during the discussions as coming from the table as a whole. The list of participants at each table were not provided. There was a consistent agreement among the participants on the day of the Open Policy Debate on the need for greater 'coordination and coherence' in combating online safety issues.[83] The need for one agency or a 'go to place' to take ownership of online safety issues was highlighted and the benefit of a structure which would allow for ongoing dialogue between Government and all stakeholders was displayed.[84] The requirement for Governmental departments to adopt responsibility for particular issues of online safety was articulated by the participants.[85] The feedback from participants from the table discussions outlined in appendix five of the report highlighted that participants generally supported the establishment of a DSC similar to the LRC recommendations. Notwithstanding the significant support, when the proposed DSC was discussed challenges with the model were also raised.[86] The balance of self-regulation and statutory regulation was one of the issues addressed. While some participants highlighted a need for a 'responsible entity' to deal directly with harmful digital content, others stated that this body or similar should only have an educational role.[87]

Towards the end of the open policy debate the discussion shifted to considering a different conception of the remit of the proposed DSC. Instead of considering the DSC as an enforcement body with the ability to provide take-down notices, consideration was given to a body with an educational and coordination role.[88] This demonstrated the difficulties in reaching agreement with regard to the role and powers of a DSC. Another notable insight from the Open Policy Debate was the reported lack of research into online safety in the Irish context. The report noted that participants highlighted that there is a 'lack of research data that is verified and verifiable, properly funded and supported'.[89]

[82] ibid Appendix B includes list of participants.
[83] ibid 10.
[84] Ibid.
[85] ibid.
[86] ibid.
[87] ibid.
[88] ibid.
[89] ibid 12.

While broad support to 'do something' was clear from the Open Policy Debate, the continued lack of consensus on the best and most appropriate means to proceed led to continued delay in legislative change.

4.2.7 The Government's Action Plan for Online Safety

On the 11th of July 2018 the Government released its Action Plan for Online Safety 2018-2019 which was informed and influenced by the Open Policy Debate on Online Safety. This was an important document as it was the first of its kind from the Irish Government. It clarified where the Government felt greater protection online was required and outlined how this protection would be achieved in its plan. The key objective of the Action Plan was to 'set out and implement actions over a short 18 month period that are achievable and which will have the greatest impact for online safety'.[90] The Action Plan was centred on five goals: 'Online Safety for All', 'Better Supports', 'Stronger Protections', 'Influencing Policy', and 'Building our Understanding'.[91] Within these five centred goals, there were 25 specific actions to be progressed over the 18 months. These 25 actions were mainly centred on education and awareness.[92] While this was a step in the right direction, it provided no remediation mechanisms and limited protections for victims, including victims of IBSA. The Action Plan was focused on short-term actions that could be taken while work on the Digital Safety Commissioner Bill 2017 progressed.[93] It was highlighted that a takedown system would require 'EU or international approaches'.[94] The Action Plan supported the self-regulation of intermediaries with three actions centred on this concept. Action 13 was intended to 'strengthen links and processes with industry for removing illegal and harmful material'[95]. Actions 14 and 15 indicated plans to 'work with online platforms based in Ireland to advance online safety measures'[96] and to 'work with industry to develop a practical guide for online platforms and interactive services to support best practice in online safety design' respectively.[97] Some commentators criticised the Action Plan for containing 'no mandatory actions'[98] against online platforms. There was also disappointment expressed in some quarters as no date was set

[90] Government of Ireland, *Action Plan for Online Safety 2018-2019,* 8.
[91] ibid.
[92] ibid actions 1-10,16,19,25.
[93] ibid 43.
[94] ibid 44.
[95] ibid 9.
[96] ibid.
[97] ibid.
[98] Kitty Holland, 'Online Proposals have no Sanctions Against Service Providers' *Irish Times* (Dublin, 11 July 2018).

for the implementation of the proposed DSC.[99] In particular the Irish Society for the Prevention of Cruelty to Children expressed strong disappointment with the Action Plan stating 'the ISPCC cannot support the approach that this plan takes in favouring self-regulation of industry over legal regulation'.[100] The former chief executive from the ISPCC Grainia Long stated that the report was 'an important piece of work' but it does not go far enough.[101]

4.2.8 The Dispatches Revelations

Perhaps one of the most significant milestones which exposed major issues for the regulation of and enforcement against IBSA in Ireland was the 'Dispatches Revelations'. On the 17th of July 2018 at 9pm, an undercover investigation by Firecrest Films for Channel 4 Dispatches programme called 'Inside Facebook: Secrets of the Social Network' aired. Channel 4 Dispatches sent an undercover reporter to work as a content moderator in Facebook's outsourced centre at CPL Resources plc in Dublin. The programme revealed for the first time how Facebook decides what users 'can and can't see' on their platform.[102] The investigation revealed the training given to content moderators to demonstrate how to decide whether content reported to them by users, such as graphic images, child abuse, self-harming, and violence should be allowed to remain on the site or be deleted. The investigation also filmed day-to-day moderation of content on the site revealing that moderators have three options – ignore, delete or mark content as disturbing which places restrictions on who can see the content.[103]

The investigation exposed how Facebook in some cases did not remove harmful digital content such as content depicting child abuse, self-harm, and violence. The investigation highlighted how conflicting motives such as profit play a particular role in why some harmful content remained online. One moderator told the Dispatches undercover reporter that 'if you start censoring too much then people lose interest in the platform . . . It's all about making money at the end of the day'.[104] This monetary motivator as a reason for allowing harmful digital content to remain on the Facebook platform was also confirmed by Rodger McNamee one of Facebook's earliest investors and a mentor to CEO Mark

[99] ibid.
[100] ibid.
[101] ibid.
[102] Channel 4 Dispatches, 'Inside Facebook: Secrets of the Social Network' (17 July 2018).
[103] ibid.
[104] ibid.

Zuckerburg. He explained that Facebook's business model relies on extreme content stating 'Facebook understood that it was desirable to have people spend more time on site if you're going to have an advertising based business, you need them to see the ads so you want them to spend more time on the site'.[105] The investigation also exposed how Facebook did not adhere to its own publicly stated aim to assess all reported content within 24 hours. During the period of the filming the investigation revealed a significant backlog. Due to the volume of reports, at one stage there was a backlog of 15,000 reports which were not assessed with some still waiting for moderation of up to five days after being reported.[106]

This programme highlighted the challenges of content moderation and how self-regulation was often failing to achieve the desired aims. The programme also highlighted the lack of control of intermediaries and the need for greater statutory regulation in Ireland. Applying the insights of the programme to the IBSA context, it is important to remember that one of the main aims of IBSA victims is to regain control of their image in a timely fashion, and the documentary highlighted how backlogs may occur when removing content. In such circumstances, even where the image is eventually removed, the damage may already be done. The harm may be irreversible at that point. Due to the public response to the documentary, it is reasonable to question whether the Government may have supported an expedited legislative response and establishment of a DSC sooner if the documentary had been released before the launch of the Action Plan for Online Safety.

4.2.8.1 Responses following the Dispatches Revelations

Following these revelations, public and media outlets voiced concerns over entrusting internet companies with online safety and strongly advocated for the establishment of a DSC.[107] Politicians expressed the need for a DSC with the power to impose fines on social media platforms for non-compliance with policies.[108] Tanya Ward from Children's Rights Alliance also expressed the need for a DSC following the Dispatches revelations stating that there is a need to 'provide real legal remedies'.[109] The then Taoiseach Leo Varadkar

[105] ibid.
[106] ibid.
[107] Barry O'Sullivan, 'Social Media Giants Must be Excluded from Online Safety Watchdog' *Irish Times* (Dublin, 21 July 2018).
[108] Ronán Duffy, 'Calls for Fines and Gardaí after Undercover Report about Facebook Moderation in Dublin' *The Journal* (18 July 2018).
[109] ibid.

announced that the introduction of fines for online companies would be considered following the revelations admitting that there was a 'failure' of self-regulation.[110] This view that social media platforms are failing to uphold their own online safety polices in Ireland was supported by the Children's Rights Alliance, the Irish Society for the Prevention of Cruelty to Children and CyberSafe.[111]

On the 1st of August 2018, the Joint Committee on Communications, Climate Action and Environment held a discussion on the moderation of violent and harmful content on the Facebook platform. Facebook was called to attend this discussion. Niamh Sweeney, Head of Public Policy at Facebook Ireland and Siobhán Cummiskey, Facebook's Head of Content Policy for Europe, the Middle East, and Africa attended the meeting. Facebook's representatives acknowledged the failure of Facebook's processes in response to harmful content and apologised stating 'much of it [the programme] did not accurately reflect Facebook's polices or values'.[112] In response to the programme, Facebook removed any harmful content identified in the programme and applied the use of media matching technology to prevent future uploads of the materials to the Facebook platform.[113] Facebook also stated that they launched an internal investigation into the processes at CPL and were taking actions to address training and enforcement of their content polices.[114] Furthermore, Facebook stated it was making changes to 'substantially increase the level of oversight' of their in-house training by Facebook policy experts and will test even further the 'readiness' of content reviewers before they review real cases.[115] Facebook also pledged to introduce new quality control measures, conduct an audit of past quality control checks, deploy spot testing, and enhance their curriculum for content reviewers to include more coaching, personalisation training, and more practice. As a direct response Facebook stated they had increased oversight at CPL, seconded Facebook employees to the CPL site, and corrected any errors in the training documentation and retrained all trainers at the CPL site.[116]

While these actions were welcome, a question remains as to whether these steps would have been taken if the Dispatches Revelations documentary did not air and receive widespread attention. While acknowledgement of Facebook's apology was evident in the

[110] Vivienne Clarke, 'Ask Facebook to Leave Ireland if it Won't Control Content' *Irish Times* (Dublin, 19 July 2018).
[111] ibid.
[112] Joint Committee on Communications, Climate Action and Environment, Moderation of violent and harmful material on the Facebook platform: Discussion (1 August 2018) 3.
[113] ibid.
[114] ibid 5.
[115] ibid.
[116] ibid 23,24.

Dáil, many politicians raised key issues around the regulation of harmful content on Facebook. Member of the opposition Labour Party Deputy Seán Sherlock stated that Facebook is one of the most scrutinised companies in the world yet is not the most regulated. He explained that there is a need for regulation as Facebook has proven to be 'incapable or unwilling to remove certain content'.[117] Independent member of the opposition, Deputy Michael Lowry highlighted that it may be impossible for Facebook to self-regulate due to the 'sheer numbers' and 'level of diversity' on the Facebook platform.[118] Deputy Michael Lowry also raised the point that if Facebook can take 'corrective action' and remove all harmful images after the Dispatches Revelations, why could the platform not resolve these sorts of issues previously.[119]

Green Party leader in opposition at the time Deputy Eamon Ryan posed the question of how many times Facebook has been prosecuted in the courts in Ireland and the UK in recent years for not removing material where someone has expressed concern or where Facebook has not removed material quickly enough.[120] Facebook responded to this question stating that they are unsure as to the number of cases before the courts. They also recognised that there are cases in which Facebook has not moved quickly enough to remove content.[121] Facebook acknowledged their lack of ability to guarantee the removal of harmful content in all cases. Facebook explained that where there is human review of content there is always the possibility of human error and therefore Facebook 'cannot tell . . . that there will be no examples of mistakes being made in the future'.[122] Facebook also pointed out that their removal of material and use of media matching technology only means that the material will not appear again on the Facebook platform but does not prevent peer-to-peer sharing or downloading of the material. Therefore, while Facebook may be able to self-regulate it does not mean other mediums will self-regulate also.[123] Facebook did accept the need for further regulation however pointed out that any regulation would need to be 'done sensibly'.[124]

A significant outcome of this discussion was Facebook's declared support for the establishment of a DSC as proposed by the LRC and Sinn Féin's Digital Safety

[117] ibid 8.
[118] ibid 18.
[119] ibid.
[120] ibid 21.
[121] ibid 26.
[122] ibid 22.
[123] ibid.
[124] ibid 34.

Commissioner Bill 2017. However, although Facebook expressed some support to the proposed DSC, Deputy Timmy Dooley questioned whether Facebook holds some 'reticence'.[125] He further made the point that this reticence had been seen through the language of the then Taoiseach Leo Varadkar.[126] He suggested that Leo Varadkar and Mr Mark Zuckerberg may have a close relationship and that this may lead to a tendency to support self-regulation policies rather than an equipped DSC. He specifically asked Facebook to disclose whether Facebook had lobbied the Government regarding the matter of appointing a DSC.[127] Facebook responded that there 'is no perceived reticence' towards the implementation of a DSC.[128] Facebook acknowledged, however, that they had highlighted the potential impact on freedom of expression.[129] It is important to note that this proposed legislation (The Digital Safety Commissioner Bill 2017) which Facebook indicated tempered support of, did not include the power to impose fines. Facebook believes that a 'multi-pronged' approach would be necessary, and that education would be pivotal.[130]

Overall, the Dispatches Revelations showed the limitation of self-regulation and the need for a statutory enforcement response. The discussion showed how intermediaries may have the ability to control harmful online content but may not choose to apply strict policies when they have a competing interest.

4.2.9 The Discord Leak

In November 2020, one of the 'largest examples of online image-based abuse in Ireland'[131] was exposed where 140,000 images of women and young girls were disseminated online without consent from a US-based server called Discord.[132] Many of

[125] ibid 31.
[126] Ellen Coyne, 'Varadkar Axed Digital Safety Officer Plan after Meeting Facebook's Mark Zuckerberg' *The Times* (Dublin, 2 August 2018).
[127] Joint Committee on Communications, Climate Action and Environment, Moderation of violent and harmful material on the Facebook platform: Discussion (1 August 2018) 31.
[128] ibid.
[129] ibid 32.
[130] ibid 6.
[131] Ellen Coyne, 'The Cowardly Backlash Against Women Who Discovered Online Campaign of Image-Based Sexual Abuse' *The Independent* (Dublin, 20 November 2020).
[132] Ellen Coyne, 'The Cowardly Backlash Against Women Who Discovered Online Campaign of Image-Based Sexual Abuse' *The Independent* (Dublin, 20 November 2020); The Editorial Board, 'The Discord Leak Was Harrowing. It Cannot Happen Again' (*University Times*, 22 November 2020); Rachel O'Connor, 'Gardaí Say 'No Evidence' Sexual Images of Irish Women Stolen' *The Irish Post* (Dublin, 26 November 2020); Órla Ryan, 'Gardaí Looking into Allegations that Large Number of Images of Women Were Shared Online Without Their Consent' (*The Journal*, 19 November 2020); Connor Gallagher, 'Garda Pessimistic About Bringing Charges Over 'Revenge Porn' Leaks' *The Irish Times* (Dublin, 21 November 2020); Aoife Moore, 'Assistant Commissioner to Lead Urgent Probe into Intimate Images Leak' *The Irish Examiner* (Dublin, 17 February 2021).

the images were taken covertly in changing rooms while others were taken from various platforms including Only Fans, Tinder, WhatsApp, and Instagram.[133] Linda Hayden, co-founder of Victims' Alliance, reported that the organisation first uncovered a file containing 11,000 images that were 'mostly of Irish women' and after multiple other files with between 5000 and 6000 images which amounted to approximately 140,000 images.[134] The incident caused major outrage on social media and as a result several campaigns, petitions and politicians called for IBSA to be made a criminal offence in Ireland. [135] The server was deleted and approximately 500 users who were involved in the sharing of the images were banned from the website. While the Gardaí opened an investigation, they were pessimistic about securing any charges due to the lack of legislation. Linda Hayden stated, 'We believe that Irish women were targeted because the perpetrators know there is no law against sharing intimate images without consent'.[136] As a result of this leak the lapsed Harassment, Harmful Communications and Related Offences Bill 2017 (previously discussed in section 4.2.3) was rushed before the Dáil by the Minister for Justice Helen McEntee and the Government committed to passing the legislation before the end of 2020. However, as candidly noted by Linda Hayden, 'they can do things quickly when things like this happen, the question needs to be asked why it took so long to do this. The bill which was first drafted back in 2017 will have taken three years to go before the Seanad'.[137]

4.2.10 Summary of the key milestones in Ireland which led to the informing of targeted legislation and the current proposals for the regulation of harmful online content

From the above discussion, it is clear there were many challenges facing the passage of legislation tackling IBSA in Ireland from 2015-2020 in spite of significant public support for action. As seen, many of the challenges related to the removal of online content and

[133] Aoife Moore, 'Assistant Commissioner to Lead Urgent Probe into Intimate Images Leak' *The Irish Examiner* (Dublin, 17 February 2021).
[134] Órla Ryan, 'Gardaí Looking into Allegations that Large Number of Images of Women were Shared Online Without their Consent' (*The Journal*, 19 November 2020).
[135] Rachel O'Connor, 'Gardaí Say 'No Evidence' Sexual Images of Irish Women Stolen' *The Irish Post* (Dublin, 26 November 2020); Megan Jr, 'Make Revenge Porn a Criminal Offence in Ireland' available at: < https://www.change.org/p/irish-justice-department-make-revenge-porn-a-criminal-offence-in-ireland?recruiter=false&utm_source=share_petition&utm_medium=twitter&utm_campaign=psf_combo_share_initial&utm_term=petition_dashboard&recruited_by_id=d26ca6b0-293a-11eb-8940-8986c7b8fb9a > accessed 16 June 2020.
[136] Órla Ryan, 'Gardaí Looking into Allegations that Large Number of Images of Women were Shared Online Without their Consent' (*The Journal*, 19 November 2020).
[137] ibid.

control of internet intermediaries were generalisable to other online harms as well. At this point, Ireland still lacked targeted legislation criminalising IBSA and victims lacked any reliable recourse. Gardaí lacked support and resources. While many stakeholders inside and outside of government recognised the need for robust laws and remedies for victims, there was also initial scepticism regarding the appropriateness of establishing a DSC. The Dispatches Revelations and the Discord Leak moved the discourse on and resulted in increased recognition of the necessity for urgent legislative action. The following sections will outline and analyse the recently enacted targeted legislation which criminalises IBSA and the current Government proposals for a new model to respond to the challenges of regulating online service providers used by third parties to distribute harmful content.

4.3 The Harassment, Harmful Communications and Related Offences Act 2020

4.3.1 Introduction

On the 28th of December 2020, the Harassment, Harmful Communications and Related Offences Act was enacted as a result of immense social and media pressure due to the 'Discord Leak'. The Act amends existing law on harmful communications and criminalises the act of IBSA in Irish law. In the context of IBSA, the Act provides for two new offences to deal with the recording, distribution or publication of intimate images without consent and provides for the anonymity of victims of those offences.[138] The Act also provides for an offence involving the distribution, publication or sending of threatening or grossly offensive communications or messages with intent to cause harm without a requirement for persistence.[139] The Act was strongly influenced by the mother of Nicole Fox 'Coco', who was abused and harassed online and as a result committed suicide. While the Act is not officially entitled 'Coco's Law', it is colloquially known as such and has been referred to as such by Government representatives in internal documents and in public presentations.[140]

4.3.2 The criminalisation of IBSA

[138] Harassment, Harmful Communications and Related Offences Act 2020, s 2, s 3.
[139] ibid s 4.
[140] Helen McEntee, Harassment, Harmful Communications and Related Offences Bill 2017: Committee Stage (1 December 2020).

In the context of IBSA, the Act creates two new offences which criminalise the non-consensual distribution of intimate images and also defines what is meant by the word 'intimate image'. Section 1 defines an intimate image as follows:

> 'intimate image', in relation to a person, means any visual representation (including any accompanying sound or document) made by any means including any photographic, film, video or digital representation—
>
> (a) of what is, or purports to be the person's genitals, buttocks or anal region and, in the case of a female, her breasts,
>
> (b) of the underwear covering the person's genitals, buttocks or anal region and, in the case of a female, her breasts,
>
> (c) in which the person is nude, or
>
> (d) in which the person is engaged in sexual activity;

Section 2 of the Act outlines the first of the new offences and deals with the distribution or publication of intimate images without consent and with the intent to cause harm or being reckless as to whether harm is caused. The penalties applicable can be an unlimited fine and/or seven years imprisonment.

Section 2 states:

> 2. (1) A person who distributes, publishes or threatens to distribute or publish an intimate image of another person—
>
> (a) without that other person's consent, and
>
> (b) with intent to cause harm to, or being reckless as to whether or not harm is caused to, the other person, is guilty of an offence.
>
> (2) For the purposes of subsection (1), a person causes harm to another person where—
>
> (a) he or she, by his or her acts, intentionally or recklessly seriously interferes with the other person's peace and privacy or causes alarm or distress to the other person, and
>
> (b) his or her acts are such that a reasonable person would realise that the acts would seriously interfere with the other person's peace and privacy or cause alarm or distress to the other person.
>
> (3) A person who is guilty of an offence under this section is liable—
>
> (a) on summary conviction to a class A fine or imprisonment for a term not exceeding 12 months, or both, or
>
> (b) on conviction on indictment to a fine or imprisonment for a term not exceeding seven years, or both.

Under this section a person who distributes or publishes an intimate image must have intended or been reckless as to whether the act would seriously interfere with the peace and privacy of the other person or cause the other person harm, alarm or distress. Furthermore Section 2 requires that a reasonable person would realise that the acts would seriously interfere with the other person's peace and privacy or cause alarm or distress to

the other person. Threatening to distribute or publish such an intimate image is also an offence.[141]

Section 3 of the Act creates the second offence and deals with the recording, distribution or publication of an intimate image without consent even if there is no specific intent to cause harm. An offence committed under this section will result in a maximum penalty of a €5000 fines and/or 12 months imprisonment.

Section 3 states:

> 3. (1) Subject to subsection (2), a person is guilty of an offence where—
> (a) he or she records, distributes or publishes an intimate image of another person without that other person's consent, and
> (b) that recording, distribution or publication, as the case may be, seriously interferes with that other person's peace and privacy or causes alarm, distress or harm to that other person.
> (2) Subsection (1) shall not apply to a person who distributes or publishes an intimate image for the purpose of the prevention, investigation or prosecution of an offence under this section.
> (3) A person who is guilty of an offence under this section is liable on summary conviction to a class A fine or imprisonment for a term not exceeding 12 months, or both

As an intention to cause harm is not required under Section 3, a person who records, distributes or publishes an intimate image without consent will be guilty of an offence where they 'seriously interferes with that other person's peace and privacy or causes alarm, distress or harm to that other person.'[142]

4.3.3 Critical Analysis of the Harassment, Harmful Communications and Related Offences Act 2020

The new legislation is a positive step towards combating online harmful communications as for the first time, after several false starts, IBSA is now clearly identified as a criminal behaviour in Ireland. A representative from An Garda Síochána, Detective Chief Superintendent Declan Daly of the Garda National Protective Services Bureau stated that the Gardaí 'will commit to investigating every report of image-based sexual abuse as a

[141] Harassment Harmful Communications and Related Offences Bill 2017, Explanatory Memorandum.
[142] ibid.

matter of priority'.[143] It is important to analyse this legislation to establish its potential effect in protecting and remedying victims of IBSA.

4.3.3.1 Definition of an intimate image

A key merit of the definition of an intimate image is that it is inclusive of all forms of images and is sufficiently technology neutral to include any advances in technology which may create other ways of creating an intimate image. Section 1 of the Act states:

> "intimate image", in relation to a person, means any visual representation (including any accompanying sound or document) made by any means including any photographic, film, video or digital representation—
>
> (a) of what is, or purports to be the person's genitals, buttocks or anal region and, in the case of a female, her breasts,
> (b) of the underwear covering the person's genitals, buttocks or anal region and, in the case of a female, her breasts,
> (c) in which the person is nude, or
> (d) in which the person is engaged in sexual activity;

The definition includes the wording 'digital representation' which can include 'photo-shopped' images that have been altered technologically by transposing a person's face onto a sexually explicit body and computer-generated images that have been completely generated by technology whereby no image of the targeted person was ever taken but rather an image is generated to look like that person.

This definition successfully covers all elements of nudity and also images whereby private areas are covered by underwear. Unfortunately, similar to the LRC definition of an intimate image under the LRC proposed model legislation outlined in section 4.2.2.1, this definition also does not expand on what is regarded as underwear. As a result, this definition may not include provocative clothing such as an image with a person fully clothed in an ensemble of a suggestive nature. For example, certain items of clothing may not be what a person would choose to wear in public yet may not be categorised as underwear or expose any of the body parts outlined in the proposed definition. It would appear that an image capturing a person posing in such clothing would not be considered 'intimate' under the proposed definition, yet if this image was posted online without

[143] Eva Wall, 'Gardai Commit to Investigate Every Report of Image-Based Abuse' (Extra.ie, 17 December 2020) < Gardai commit to investigate every report of image-based abuse - Extra.ie > accessed 22 February 2022.

consent the harm could be equivalent regardless of the lack of nudity or sexual activity. For example, the Australian Online Safety Act 2021 specifically makes reference to an image of a person without their religious attire as amounting to an intimate image. This should be considered in the Irish context. It remains to be seen how the Irish courts interpret this definition should a situation like the above occur.

4.3.3.2 Issues with the requirement to 'seriously interfere'

As set out above, in order to be convicted under Section 2, a person who shares an intimate image without consent must either intend to cause harm or be reckless as to whether they have caused harm. A person will be deemed to cause harm where they intentionally or recklessly seriously interfere with the other person's peace and privacy or causes alarm or distress to the other person, and a reasonable person would realise that the acts would seriously interfere with the other person's peace and privacy or cause alarm or distress to the other person. Section 3 does not require that a person who records or shares an intimate image without consent to have intended to or been reckless as to whether their actions caused harm. Instead, a person can be found guilty under Section 3 where the relevant 'recording, distribution or publication' seriously interferes with the target's 'peace and privacy or causes alarm, distress or harm to that other person'.

The use of the word 'seriously' creates a potential barrier for victims when considering making a complaint. Victims may trivialise their experience and feel it is not worth reporting as it may not reach the level of seriousness potentially expected from the law. Furthermore, McGlynn highlighted that many victims do not necessarily want to admit that their experience of IBSA has had a serious impact on them.[144] As a result, requiring that the act 'seriously' interferes with another person, creates a potentially barrier for victims in reporting an offence.

Another question which arises is how is a serious interference with another's peace and privacy to be proven? If the intimate image is shared with a small number of people, the impact of such an act may be trivialised and minimised and as a result it may not be regarded as a serious interference. McGlynn and Rackley highlight how such thresholds hinder prosecutions as police and prosecutors are reluctant to take cases forward as they

[144] Nicola Henry, Clare McGlynn, Asher Flynn, Kelly Johnson, Anastasia Powell, & Adrian Scott, '*Image-Based Sexual Abuse: A Study on the Causes and Consequences of Non-Consensual Nude or Sexual Imagery*' (1st edn, Routledge 2020); Clare McGlynn, Erika Rackley, Kelly Johnson, Nicola Henry, Nicola Gavey, Asher Flynn, Anastasia Powell, & Adrian Scott, 'Shattering Lives and Myths: A report on Image-Based Sexual Abuse' (2019) *Project Report. Durham University; University of Kent*.

become more difficult to support when they have to prove a threshold of seriousness.[145] Often police resort to an informal response to a complaint for example, by issuing informal requests that images be taken down or by giving the perpetrator an informal caution or warning instead of bringing a criminal case.[146] In cases where the police believed the abuse did not amount to a crime, or where they felt there was not enough evidence to prosecute, this informal approach was taken instead.[147] Eliminating the need to prove a threshold of seriousness may avoid the creation of a barrier to prosecutions in Ireland as seen in other jurisdictions such as the UK, Australia, and New Zealand. It is important that Ireland does not create an 'ideal' type of victim and removes the need to prove a level of seriousness as this threshold is too subjective.

Furthermore, the alternative of requiring proof of 'actual alarm, distress or harm' is also concerning. The providing of evidence to prove harm caused may traumatise the victim and may lead to the victim having to expose more private intimate information. Experiences recorded from New Zealand by McGlynn, Rackley and Johnston highlighted how such a requirement to prove actual harm re-traumatises victims making them reluctant to report.[148]

4.3.3.3 Issues with the need to prove intent

Section 2 of the Harassment, Harmful Communications and Related Offences Act 2020, which carries the more serious penalty of 7 years, will only find a person guilty of an offence where the offending image is shared 'with intent to cause harm to, or being reckless as to whether or not harm is caused to, the other person'. This emphasis on the perpetrator's motives can seriously constrain the ability of a victim to successfully prosecute their perpetrator for the more serious crime.[149]

---

[145] Clare McGlynn, Erika Rackley, Kelly Johnson, Nicola Henry, Nicola Gavey, Asher Flynn, Anastasia Powell, & Adrian Scott, 'It's Torture for the Soul": The Harms of Image-Based Sexual Abuse' (2020) 30(4) Social and Legal Studies 541.

[146] Clare McGlynn, Erika Rackley, Kelly Johnson, Nicola Henry, Nicola Gavey, Asher Flynn, Anastasia Powell, & Adrian Scott, 'Shattering Lives and Myths: A Report on Image-Based Sexual Abuse' (2019) *Project Report. Durham University; University of Kent*; Nicola Henry, Clare McGlynn, Asher Flynn, Kelly Johnson, Anastasia Powell, & Adrian Scott, '*Image-Based Sexual Abuse: A Study on the Causes and Consequences of Non-Consensual Nude or Sexual Imagery*' (1st edn, Routledge 2020).

[147] ibid.

[148] Clare McGlynn, Erika Rackley, Kelly Johnson, Nicola Henry, Nicola Gavey, Asher Flynn, Anastasia Powell, & Adrian Scott, 'Shattering Lives and Myths: A Report on Image-Based Sexual Abuse' (2019) *Project Report. Durham University; University of Kent.*

[149] Clare McGlynn & Erika Rackley E, 'Image-Based Sexual Abuse' (2017) 37 Oxford Journal of Legal Studies 534.

While the paradigmatic 'revenge porn' case may involve a declared intention to cause distress, images are distributed for a wide variety of reasons including financial gain, notoriety, amusement or sexual gratification and may not have any intent to cause harm to a victim. Furthermore, in some cases the distributors of the intimate image do not know the identity of the person in the image or have no intention of the victim-survivor finding out the image of him/her was taken or shared.[150] In these cases Section 2 which carries the more serious penalty would be challenging to apply. For example, would the scandal of the Discord leak discussed in section 4.2.9 be covered under this law? It seems plausible that it would only be possible under the less serious offence of Section 3 which does not require intention. As a result, it is likely that participants in a future scandal similar to the Discord leak would only be liable for a custodial sentence of a maximum of 12 months. This does not seem like the serious criminal sanctions that the Government have been talking about in the lead up to the implementation of the Harassment, Harmful Communications and Related Offences Act. While it is necessary to have two offences so to account for crimes of different gravity especially in situations where there is no element of maliciousness, the small penalty associated with Section 3 fails to acknowledge the harm that is still caused to the victims regardless of the lack of intent or recklessness.

4.3.3.4 Issues with the lack of consideration for 'recording' in section 2

As noted in section 4.3.2, IBSA is criminalised under section 2 and section 3 of the Harassment, Harmful Communications and Related Offences Act 2020, with section 2 carrying a more extensive penalty including a maximum term of imprisonment of up to 7 years as compared to a maximum term of imprisonment of up to 12 months under section 3. Section 2 only considers cases whereby an image has been distributed, published or threatened to be distributed or published. The covert or non-consensual recording of an intimate images which is not further disseminated but may be stored on a device or visually shown to other people while stored on that device is not included under this section. While the recording of an intimate image without consent is covered under section 3, penalties for such an act are capped at a summary conviction. The recording of an intimate image without consent even if not further disseminated is a serious breach of

[150] ibid.

a person's sexual privacy. The exclusion of this act from section 2 minimises the behaviour and potential harm caused to a victim and therefore should be consider for inclusion in section 2 also.

Overall, while the criminalisation of IBSA in Ireland is a positive step, the law is not without limitations and it remains to be seen how the courts will apply and interpret the law around challenges such as proving the serious nature of the act, the harms caused to the victim, and the intent or recklessness of the perpetrator to cause serious harm. Furthermore, while the implementation of two criminal offences satisfies the need for targeted legislation against IBSA, it only provides for the prosecution of the perpetrator. This is often a secondary priority of victims of IBSA, who often place most value on the removal of the images from the internet.[151]

4.4 Application of the victim-centred framework to the Irish situation up to and including the Harassment, Harmful Communications and Related Offences Act 2020

In order to assess the Irish developments in the area of IBSA from a victim-centred perspective, it is necessary to apply the framework initially developed in Chapter 2 and refined in Chapter 3. Applying the victim-centred framework allows the author to assess how well the Irish legal system addressed the needs of victims of IBSA prior to the enactment of the OSMRA. Understanding the strengths and weaknesses of the Irish response up until this point provides important background to the development of the OSMRA and assists with the assessment of whether the subsequent changes to the law adequately address the needs of victims. To recall, the refined framework as applied to the Australian situation is reprinted below:

[151] Nicola Henry, Asher Flynn & Anastasia Powell (2018) 19 'Policing Image-Based Sexual Abuse: Stakeholder Perspectives', Police Practice and Research 565.

Identified needs of victims of IBSA

	Independent specialist authority	*Individual complaints mechanism*	*Removal orders*	*Orders reducing visibility of IBSA material*	*Statutorily supported codes of practice*	*Educational campaigns*	*Civil avenues of redress*	*IBSA recognition as a criminal offence*
Constraining distribution of the image	OESC - Online Safety Act 2021, s 26	IBA Portal - Online Safety Act 2021, Division 3	Compliance Notices: Service Provider Notifications - Online Safety Act 2021, s 85), Removal Notices - Online Safety Act 2021, s 77		Basic Online Safety Expectations Online Safety - Basic Online Safety Expectations) Determination 2022		Civil remedies, including damages and injunctive relief available	Criminal Code Act 1995 s 474.17(A)
Effective alternatives to constraining IBSA images	OESC - Online Safety Act 2021, s 26	IBA Portal - Online Safety Act 2021, Division 3		Link Deletion Notices – Online Safety Act 2021, s 124 and App Removal Notices - Online Safety Act 2021, s 128				
Adequately trained and resourced authorities	OESC - Online Safety Act 2021, s 26					'ThinkUKnow' campaign and 'Safe Sexting: No Such Thing' campaign		
Prompt action	OESC - Online Safety Act 2021, s 26	IBA Portal - Online Safety Act 2021, Division 3	Compliance Notices: Service Provider Notifications - Online Safety Act 2021, s 85), Removal Notices - Online Safety Act 2021, s 77	Link Deletion Notices – Online Safety Act 2021, s 124 and App Removal Notices - Online Safety Act 2021, s 128	Basic Online Safety Expectations Online Safety - Basic Online Safety Expectations) Determination 2022			
Empowerment	OESC - Online Safety Act 2021, s 26	IBA Portal - Online Safety Act 2021, Division 3				'ThinkUKnow' campaign and 'Safe Sexting: No Such Thing' campaign		Criminal Code Act 1995 s 474.17(A)
Confidentiality	OESC - Online Safety Act 2021, s 26	IBA Portal - Online Safety Act 2021, Division 3						

Figure 13 Refracted framework table of key needs and identified tools/mechanisms in the Australian context following the enactment of the Online Safety Act 2021 as developed in Chapter 3

It is useful to bear this in mind when considering how the Irish situation (prior to the OSMRA) addressed the needs of IBSA victims. The qualitative research conducted in Chapter 3 confirmed that the various tools/mechanisms identified in Chapter 2 have the potential to respond to the needs of IBSA victims, at least in part. For clarity and ease of comparison, the refined framework is printed below without reference to specific laws in order to indicate what tools/mechanisms respond to which victim needs as informed by

the Australian experience. This abstract framework is then used to consider how the Irish system (prior to the OSMRA) responds to the needs of victims of IBSA. The analysis is informed by comparison with the Australian system.

Identified tools/mechanisms that address the needs of victims of IBSA

Identified needs of victims of IBSA	*Independent specialist authority*	*Individual complaints mechanism*	*Removal orders*	*Orders reducing visibility of IBSA material*	*Statutorily supported codes of practice*	*Educational campaigns*	*Civil avenues of redress*	*IBSA recognition as a criminal offence*
Constraining distribution of the image	+	+	+		+		+	+
Effective alternatives to constraining IBSA images	+	+		+				
Adequately trained and resourced authorities	+					+		
Prompt action	+	+	+	+	+			
Empowerment	+	+				+		+
Confidentiality	+	+						

Figure 14 Framework table illustrating the relationship between the needs of IBSA victims and the potential tools/mechanisms as informed by the Australian experience

Out of the eight identified tools/mechanisms, the Irish response prior to the OSMRA provided for three tools/mechanisms that responded in some way to the needs of IBSA victims. These tools/mechanisms were educational campaigns, civil avenues of redress and the recognition of IBSA as a criminal offence.

In 2017, McGlynn and Rackley identified the need for greater educational and prevention campaigns to highlight the issues of IBSA within Ireland.[152] The Government's Action Plan for Online Safety 2018-2019 recognised the importance of such campaigns. As outlined in section 4.2.7, the Action Plan for Online Safety was centred on five goals: 'Online Safety for All', 'Better Supports', 'Stronger Protections', 'Influencing Policy', and 'Building our Understanding'.[153] Within these five centred goals, there were 25 specific actions to be progressed which were mainly centred on education and awareness.[154] Examples of such campaigns initiated by both Government and non-

[152] Clare McGlynn and Erika Rackley, 'More than "Revenge Porn": Image-Based Sexual Abuse and the Reform of Irish Law' (2017) 14 Irish Probation Journal.
[153] ibid.
[154] ibid actions 1-10,16,19,25.

governmental organisations which arose following the Action Plan include: 'Be Safe Online', 'Same Rules Apply' Online Safety Campaign, and '1 2 3 Online Safety Campaign'.[155]

In Ireland, victims may also seek damages and/or injunctive relief through traditional civil avenues as outlined in Chapter 1.[156] They may do this through civil actions founded on established law with application in the IBSA context. Depending on the circumstances, areas of law which may have application in a particular case may include privacy law, data protection law, copyright law, defamation law, and harassment law.

A more recently adopted mechanism evident in the Irish context prior to OSMRA is the recognition of IBSA as a criminal offence under section 2 and section 3 of the Harassment, Harmful Communications and Related Offences Act 2020 as discussed above in section 4.3. An additional tool/mechanism that responds to the needs of victims is provided for in the form of Hotline.ie.[157] Hotline.ie is a non-profit national reporting mechanism through which members of the public can report concerns in respect of illegal content online.[158] Originally this reporting tool mainly dealt with child sexual abuse material however with the criminalisation of IBSA in 2020 under the Harassment, Harmful Communications and Related Offences Act 2020, reports of IBSA now fall under the scope of this reporting mechanism. In September 2021, Hotline.ie launched its secure and confidential 'Intimate Image Abuse web-reporting portal and service', which

[155] Government of Ireland, 'Be Safe Online' < gov.ie - Be Safe Online (www.gov.ie)> accessed 2 May 2023; National Parents Council and CyberSafeKids, 'Same Rules Apply' 'Same Rules Apply - CyberSafeKids' accessed 2 May 2023; Children's Rights Alliance, '1 2 3 Online Safety Campaign' < 1 2 3 Online Safety Campaign | Children's Rights Alliance (childrensrights.ie)> accessed 2 May 2023.

[156] Chapter 1 section 1.5

[157] The Hotline web-reporting service was launched in November 1999, to fulfil one of the key recommendations of the Irish Government Working Group on the Illegal and Harmful Use of the Internet (1998). The operations and procedures of Hotline.ie are agreed and overseen by the Department of Justice and Equality. Hotline.ie works closely with a diverse 'mix of Government and inter-governmental agencies, law enforcement, online service providers and NGOs' Hotline.ie, *Break the Cycle One Report at a Time* (Annual Report 2020). Hotline.ie a founding member of INHOPE (the International Association of Internet Hotlines) and works in collaboration with 46 other hotlines worldwide to ensure the swift removal of child sexual abuse material. Hotline.ie, 'Who We Are' < Hotline.ie - About Us > accessed 2 May 2023. The Hotline.ie Code of Practice outlines the framework for collaboration between Hotline.ie, member online service providers, and law enforcement for the purpose of countering illegal content online, especially child sexual abuse material. Hotline.ie, *Code of Practice* Countering the Availability and Proliferation of Illegal Content Online, Namely Child Sexual Abuse Material (May 2020). As of 2020 Hotline.ie has 27 members including BT, HEAnet, Three Ireland, Virgin Media, Google Ireland, Eir, Vodafone, Sky, APTUS, Blacknight, HostingIreland.ie, Imagine, Irishdomains.com, Westnet, Tesco mobile, Airwave Internet, ARRA Communications, Atlanktek Computers, ECHO Broadband, KB, Nova Broadband, Nuwave Rural Broadband, Orion, Spiral Hosting, Wireless Connect and Sterncov.

[158] Hotline.ie, 'Who We Are' < Hotline.ie - About Us > accessed 2 May 2023.

was developed in conjunction with the Department of Justice and An Garda Síochána.[159] Hotline.ie now assists IBSA victims with the 'reporting and removal of intimate images', 'by liaising with An Garda Síochána should the reporter wish to have the matter investigated by the Gardaí' and by 'signposting to relevant resources and other support services available in Ireland' including, for example, Women's Aid.[160] If the material reported to Hotline.ie is deemed to be illegal material that can be traced to Ireland, Hotline.ie notifies An Garda Síochána and also notifies the appropriate online service provider (if a member) which is responsible for the removal of the specified content from the internet.[161] The Hotline Code of Practice defines the Notice and Takedown Procedure under which members are:

> requested to remove or disable (or otherwise permanently disrupt) access to potentially illegal content which is hosted on their networks, and where such content is accessible in or from Ireland, and preserve forensic evidence for law enforcement investigations.[162]

Following notification, internet service providers and hosts are obliged to remove or disable access to illegal content.[163] Where the online service provider is not a member, Hotline.ie will only notify the nominated An Garda Síochána unit, highlighting that the provider/facilitator of content is a non-member.

4.4.1 Assessing how well the identified victim needs were addressed prior to the Online Safety and Media Regulation Act 2022

Constraining distribution of the image

Prior to the OSMRA, the identified victim need of constraining the distribution of IBSA material was addressed through the tools/mechanisms of civil avenues of redress, the recognition of IBSA as a criminal offence, and through the non-profit national reporting mechanism Hotline.ie. Similar to the Australian context, civil awards of damages compensate victims for some of the harm they have suffered. However, as identified by

[159] Hotline.ie, *'People…Not Pixels'* (Annual Report 2021).
[160] ibid.
[161] Hotline.ie, *Code of Practice* Countering the Availability and Proliferation of Illegal Content Online, Namely Child Sexual Abuse Material (May 2020).
[162] ibid; As of 2020, Hotline.ie has 27 members including BT, HEAnet, Three Ireland, Virgin Media, Google Ireland, Eir, Vodafone, Sky, APTUS, Blacknight, HostingIreland.ie, Imagine, Irishdomains.com, Westnet, Tesco mobile, Airwave Internet, ARRA Communications, Atlanktek Computers, ECHO Broadband, KB, Nova Broadband, Nuwave rural broadband, Orion, Spiral Hosting, wireless connect and Sterncov.
[163] See the discussion of the e-Commerce Directive 2000/31/EC (liability of intermediary service providers) – as transposed into Irish law by the European Communities (Directive 2000/31/EC) Regulations 2003 (S.I. 68/2003) – in Chapter 1.

Walley in the Irish context, 'takedown, not damages is the main focus' of victims.[164] As a result, a potential award of damages fails to address what has been identified as the priority need of victims, the 'immediate takedown of the online material, and to take back control of the images'.[165]

As evident in the Australian context, the recognition of IBSA as a criminal offence is a positive development that may help to address victims needs to constrain the distribution of their image. Criminalising IBSA has the potential to deter possible offenders from distributing IBSA and it also provides a strong incentive and legal basis for platforms to remove IBSA material. The Harassment, Harmful Communications and Related Offences Act 2020 criminalises IBSA and attaches a significant maximum penalty of seven years imprisonment for offences committed under section 2.

The role played by Hotline.ie also responds to the need of victims to bring about the constraint of their image distribution. For example, in 2021, Hotline received 773 'intimate image abuse' reports. Out of the 773 reports made, the image was successfully removed in 490 cases following a request by Hotline.ie to service providers to remove the image.[166] However, while this mechanism can request the removal of IBSA material it has no power to force the request. For example, in 2021, out of the 773 reports made, 248 reports were deemed 'non-actionable' meaning the reports either related to 'environments or situations outside the scope/remit' of Hotline.ie, such as 'intimate images sent over encrypted or private communications' whereby the only course for removal of the imagery would be its deletion from a personal device such as a mobile phone or laptop.[167] Other examples of situations where Hotline.ie may be unsuccessful in bringing about the removal of content include where an online service provider is unresponsive, where the country the website is hosted does not criminalise IBSA and the service provider does not believe it is obliged to comply with Irish law, and where the reporter of the image provides non-functioning contact details.[168] While Hotline.ie fulfils the role of an individual complaints mechanism by allowing IBSA victims to report their case directly and seek help in removing their image, Hotline.ie has limited ability to assist in the removal of intimate images as it fails to have the necessary statutory authority to

[164] Pauline Walley, *'*In Memory Amore: Revenge, Sex and Cyberspace' (2015) 20(2) The Bar Review 33.
[165] ibid.
[166] Hotline.ie, *'People…Not Pixels'* (Annual Report 2021)25.
[167] ibid.
[168]ibid, 26.

issue a removal notice similar to the Australian IBA portal. As a result, while Hotline.ie assists in the constraining of intimate images it still faces challenges and a more empowered individual complaints mechanism is necessary.

Effective alternatives to constraining IBSA images

Prior to the OSMRA, Irish law provided for no equivalent to the Australian link deletion notices or app removal notices.[169] Accordingly, Irish law failed to provide an effective alternative mechanism for constraining the distribution of IBSA images.

Adequately trained and resourced authorities

As discussed under section 4.2.6, representatives from An Garda Síochána identified that they lacked sufficient resources and training to deal with online issues such as IBSA. While educational campaigns exist in Ireland, these campaigns are focused on societal awareness raising and equipping parents to tackle online issues experienced by their children. Hotline.ie partly addresses the need for an adequately trained and resourced authority as it has a specific mandate to tackle illegal content online and receives funding from the European Union through grant aid under the Connecting Europe Facility: Safer Internet Programme and by members including search providers, mobile operators, hosting and internet service providers.[170] Hotline.ie utilises its resources and expertise to assist and encourage the removal of child sexual abuse material and other illegal content such as IBSA.[171]

Prompt action

While figures are not reported on the timeframes for removal following removal requests by Hotline.ie, the ability to directly report an issue of IBSA to Hotline.ie instead of engaging in traditional criminal and civil avenues of redress (which are time consuming and costly) is noteworthy.

Empowerment

The recognition of IBSA as a criminal offence has the potential to have an empowering effect for victims by clearly identifying IBSA as a wrong that is not accepted by society. Providing for this in the Harassment, Harmful Communications and Related Offences

[169] Online Safety Act 2021, s 124 and s 128.
[170] Hotline.ie, *'People…Not Pixels'* (Annual Report 2021)2.
[171] ibid.

Act 2020 was an important step in the Irish response to IBSA. As discussed in Chapter 2, educational campaigns educate the broader public,[172] provide preventive messaging, [173] inform victims of their redress options, and reduce victim blaming attitudes.[174] Victims become more empowered as they are educated in the options available to them and also feel more supported in their pursuit of redress. The Irish educational campaigns prior to the Harassment, Harmful Communications and Related Offences Act 2020 did not directly discuss the options available to victims of IBSA.

Hotline.ie also addresses the need for empowerment as this mechanism offers an additional avenue of redress that is direct, 'confidential and secure'.[175] Hotline.ie also empowers victims to decide the pathway of their case once reported to Hotline.ie. A reporter of an intimate image to Hotline.ie can choose to allow Hotline.ie to liaise with An Garda Síochána should he/she want the matter investigated. [176] Notably, in the IBSA context, '[o]nly 1 in 7 reporters indicated they wished to have the matter referred to An Garda Síochána for law enforcement investigations. The vast majority opted for content removal only'.[177] Furthermore, Hotline.ie also connects victims to support services such as Women's Aid, Rape Crisis Network Ireland, Safe Ireland, Men's Aid, and Crime Victims Helpline.ie.[178] This equips victims to seek redress and receive emotional support that can assist victims to regain control of their lives.[179]

Confidentiality

Unlike the Australian system where the traditional avenues of redress as provided by the systems of criminal justice and civil law generally require the public identification of victims, the Irish criminal law provides anonymity to victims in relevant circumstances. The Harassment, Harmful Communications and Related Offences Act 2020 creates new offences in relation to harassment and harmful communications, both online and offline,

[172] Nicola Henry and Asher Flynn, 'Image-Based Sexual Abuse: Online Distribution Channels and Illicit Communities of Support' (2019) 25 Violence against Women 1950.
[173] Asher Flynn, Elena Cama and Adrian J Scott, 'Preventing Image-Based Abuse in Australia: The Role of Bystanders' Report to the Criminology Research Advisory Council Grant: CRG 02/18–19 (August 2022).
[174] Asher Flynn and Nicola Henry, 'Image-Based Sexual Abuse: An Australian Reflection' (2019) Women and Criminal Justice 322.
[175] Hotline.ie, *'People…Not Pixels'* (Annual Report 2021) 2.
[176] Hotline.ie, *'People…Not Pixels'* (Annual Report 2021) 24.
[177] Hotline.ie, *'People…Not Pixels'* (Annual Report 2021) 28.
[178] Hotline.ie, *'People…Not Pixels'* (Annual Report 2021) 30.
[179] Erika Rackley, Clare McGlynn, Kelly Johnson, Nicola Henry, Nicola Gavey, Asher Flynn and Anastasia Powel, 'Seeking Justice and Redress for Victim-Survivors of Image-Based Sexual Abuse' (2021) 29 Feminist Legal Studies 312; Nicola Henry, Asher Flynn and Anastasia Powell, 'Image-based sexual abuse: Victims and perpetrators' (2019) 572 Trends & Issues in Crime and Criminal Justice 15; Australian Government Department of Communications and the Arts, Review of the Enhancing Online Safety Act 2015 and the Online Content Scheme – discussion (June 2018) 4.

including IBSA and provides for the anonymity of victims of those offences. In particular, if a person is prosecuted under section 2 or section 3 which criminalises IBSA, the alleged victim is granted anonymity under section 5 and therefore cannot be named or identified. Unless a court allows the publication of the identity of the alleged victim, any person who names or publishes any information likely to identify the alleged victim may also be prosecuted for a criminal offence under section 5. McGlynn and Rackley identify the importance of anonymity for victims of IBSA stating, 'anonymity is vital in order to increase police reports and successful prosecutions, as well as to protect complainants from further harm'.[180] The Harassment, Harmful Communications and Related Offences Act 2020 acknowledges this need.

In recent years, Irish law and policy has increasingly recognised the harms caused by IBSA and the passage of the Harassment, Harmful Communications and Related offences Act 2020 is the clearest example of this. The analysis above shows, however, that this response did not sufficiently address the key needs of victims as identified in this thesis. In order to illustrate how well the Irish response addresses the needs of victims of IBSA following the enactment of the Harassment, Harmful Communications and Related Offences Act 2020, but prior to the enactment of the OSMRA, the table below has been populated with specific reference to Irish law and policy. The specific tools/mechanisms included have been determined to respond, at least in part, to the needs of victims.

The enactment of the Harassment, Harmful Communications and Related Offences Act 2020 was an important step forward in providing recognition of IBSA as a criminal offence. A notable effect of IBSA being declared illegal was the falling of IBSA material under the scope of the responsibility of Hotline.ie. As noted above, Hotline.ie provides a limited form of individual complaints scheme that can facilitate the voluntary removal of content from cooperative online platforms. However, it is clear that the complaints scheme is much more limited than the system in operation in Australia and thus it cannot be considered directly comparable. Nevertheless, it does represent an important improvement subsequent to the enactment of the Harassment, Harmful Communications and Related Offences Act 2020 which is why it is represented on the table. Another notable addition to the table is the recognition of the desire expressed by some victims of IBSA for anonymity in the criminal justice system. Unlike in the Australian system,

[180] Clare McGlynn and Erika Rackley, 'More than 'Revenge Porn': Image-Based Sexual Abuse and the Reform of Irish Law' (2017) 14 Irish Probation Journal.

section 5 of the Harassment, Harmful Communications and Related Offences Act 2020 makes provision for victim anonymity. In spite of this progress, the sparsely populated columns and rows indicate the clear need for improvement in the Irish response. In particular, the lack of an independent specialist authority with statutory power to issue removal orders and administer an individual compliant mechanism similar to the OESC is a notable limitation of the Irish regulatory response prior to the enactment of the Online Safety and Media regulation Act 2022. Furthermore, the Irish response fails to address the need of victims for an effective alternative avenue of redress where removal of the intimate image is impossible. Finally, the Irish response is limited in the tools/mechanisms provided and fails to administer any form of systemic governance through statutorily supported codes of practice.

Identified needs of victims of IBSA

	Independent specialist authority	*Individual complaints mechanism*	*Removal orders*	*Orders reducing visibility of IBSA material*	*Statutorily supported codes of practice*	*Educational campaigns*	*Civil avenues of redress*	*IBSA recognition as a criminal offence*
Constraining distribution of the image		Hotline.ie (limited powers and authority)[181]					Civil remedies, including damages and injunctive relief available	Harassment, Harmful Communications and Related Offences Act 2020, s 2 & s 3
Effective alternatives to constraining IBSA images								
Adequately trained and resourced authorities		Hotline.ie (limited powers and authority)[182]				Action Plan for Online Safety 2018/2019 – Action 1-5, 8, 9		
Prompt action		Hotline.ie (limited powers and authority)[183]						
Empowerment		Hotline.ie (limited powers and authority)[184]				Action Plan for Online Safety 2018/2019 – Action 1-5, 8, 9		Harassment, Harmful Communications and Related Offences Act 2020, s 2 & s 3
Confidentiality								Harassment, Harmful Communications and Related Offences Act 2020, s 5

Figure 15 Framework table of key needs and identified tools/mechanisms applied in the Irish context prior to the enactment of the Online Safety and Media Regulation Act 2022

[181] Hotline.ie is a non-profit national reporting mechanism whereby members of the public can report concerns in respect of illegal content online. It has the power to inform service providers of the existence of suspected IBSA on their platform who may voluntarily remove the material as a result. They also refer suspected IBSA to An Garda Siochana.

[182] ibid.

[183] ibid.

[184] ibid.

4.5 Introduction to the General Scheme of the Online Safety and Media Regulation Bill 2019

On the 4th of March 2019, the then Minister for Communications Richard Bruton announced that he would introduce a new law to regulate harmful online content.[185] He acknowledged how digital technology is transforming the world and that the digital world presents new risks. As a result, Bruton stated that self-regulation is no longer sustainable and that a new Online Safety Act is necessary. Bruton explained that the new OSMRB would set a 'clear expectation for service providers to take reasonable steps to ensure the safety of the users of their service' and would establish an Online Safety Commissioner within a newly established Media Commission to oversee the new system.[186] The General Scheme of the OSMRB was subsequently published. It was the intention of the General Scheme to also transpose the EU Audiovisual Media Services Directive (AVMSD) which governs EU-wide coordination of national legislation on all audiovisual media, both traditional TV broadcasts and on-demand services.[187] Bruton stated that the proposed legislation is part of a 'new era of accountability' as to date, online services have been largely self-regulating in this area, setting their own safety measures and not being externally accountable under law.[188] The proposed law represented a significant challenge for online service providers many of which have their EU Headquarters in Ireland. While the deadline for nations to transpose the EU AVMSD into legislation was the 19th of September 2020, the legislation is yet to be passed. However, the Government has stated that it hopes to implement this legislation at the 'earliest possible date' and it remains a priority for the current Minister for Tourism, Culture, Arts, Gaeltacht, Sport and Media,

[185] Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media, 'Regulation of Harmful Online Content and the Implementation of the revised Audiovisual Media Services Directive' (6 September 2020) < https://www.gov.ie/en/consultation/430d0-regulation-of-harmful-online-content-and-the-implementation-of-the-revised-audiovisual-media-services-directive/> accessed 22 February 2022.
[186] ibid.
[187] Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities.
[188] Stephen McDermott, 'Internet Companies Who Break Online Safety Rules Could be Blocked in Ireland Under New Law' (*The Journal*, 10 January 2020) < https://www.thejournal.ie/online-safety-commissioner-proposed-law-4960340-Jan2020/ > accessed 22 February 2022.

Catherine Martin who published the full version of the Bill in January 2022 (discussed below).[189] The OSMRB introduced a new system for the regulation of harmful online content in Ireland and also updates the existing regulatory systems for Television Broadcasting Services and On-demand Audiovisual Media Services such as the RTÉ Player or Apple's film & TV store.

The following sections will provide a general overview of the OSMRB with a particular emphasis on how the OSMRB impacts IBSA. The development of the general scheme of the Bill will be discussed, the structure and functions of the Media Commission will be briefly outlined, and the functions and powers of the OSC will be discussed in the context of IBSA. Stakeholder submissions, Oireachtas debates, and the Report of the Joint Committee on the Pre-Legislative Scrutiny of the General Scheme of the OSMRB will be analysed and the merits and limitations of the OSC as proposed under the OSMRB will be assessed.

Following this, the OSC as proposed under the OSMRB will be compared and contrasted to the Australian OESC informed by the insights drawn from the interviews discussed in Chapter 3. Based on this analysis recommendations will be made.

4.5.1 Development of the General Scheme of the Online Safety and Media Regulation Bill 2019

Before outlining the functions and powers under the general scheme of the OSMRB, it is important to understand the development of the general scheme of the Bill and what informed its draft state in the context of IBSA. In order to inform the drafting of the General Scheme of the proposed legislation, the Government conducted a public consultation, prepared a series of policy papers, and engaged with key stakeholders.

4.5.1.1 Public Consultation

A public consultation was held between the 4th of March and the 15th of April 2019. This public consultation aimed to seek the views of citizens and stakeholders as to an achievable, proportionate and effective approach to regulating harmful content, particularly online. People and organisations were invited to respond to 16 questions set

[189] Dáil Éireann Debate, 'Proposed Legislation' (4 July 2019) < https://www.oireachtas.ie/en/debates/question/2019-07-04/50/ > accessed 22 February 2022.

out in an online form[190] which was accompanied by an explanatory note.[191] These questions were asked under four strands which represented the different services and regulatory systems to be established or updated.[192] For the purpose of this thesis 'strand 1' is of most relevance as it focused on national regulatory measures to improve online safety. The questions here focused on 'what oversight systems could be put in place to ensure that online platforms improve how they deal with and remove 'harmful online content', what kinds of material should be considered 'harmful online content' and what kinds of online services should be covered by this system'.[193] In total, 84 submissions were received from a wide range of stakeholders, including members of the public, commercial organisations and industry groups, public bodies, and NGOs. Of these responses, 40 were from members of the public, 21 were from commercial organisations and industry groups, 7 were from public bodies and 16 were from NGOs.[194] These submissions were published on the Department's website on the 27th of June 2019. The Government stated that 'the submissions will provide an important input into the ongoing development of an Online Safety and Media Regulation Bill.'[195]

A thematic analysis of the consultation responses was published on the 25th of July 2019. General feedback from the submissions highlighted the need for 'consistency' in legislation and regulation, that legislation and regulation should be 'future-proofed' to the greatest extent possible and that 'legal safeguards' are needed in legislation to prevent 'unintended consequences' and to avoid imbalances in the consideration of rights.[196] In particular the submissions identified the need for the legislation to be drafted within a clear 'rights based framework' and that 'right balancing exercises' would be essential to any regulatory system established.[197] This particularly related to the right to freedom of

[190] Department of Communications, Climate Action & Environment, *Public Consultation on the Regulation of Harmful Content on Online Platforms and the Implementation of the Revised Audiovisual Media Services Directive.*
[191] Department of Communications, *Climate Action & Environment, Public Consultation on the Regulation of Harmful Content on Online Platforms and the Implementation of the Revised Audiovisual Media Services Directive Explanatory Note.*
[192] Strand 1 - National Online Safety System (The first strand of the consultation is about what national regulatory measures to improve online safety should be put in place.), Strand 2 - Audiovisual Media Services Directive- Video Sharing Platforms (The second strand of the consultation is about how Ireland should implement the new EU rules for Video Sharing Platform Services (VSPS) located in Ireland.), Strands 3 and 4 - Audiovisual Media Services Directive (Ondemand Audiovisual Media Services and TV) (The third and fourth strands are about how Ireland should implement the new EU rules for On-demand Audiovisual Media Services and TV services located in Ireland.)
[193] Department of Communications, Climate Action & Environment, *Thematic Analysis - Public Consultation on the Regulation of Harmful Online Content and the Transposition of the Audiovisual.*
[194] ibid.
[195] ibid.
[196] ibid 9.
[197] ibid 14.

expression. The responses also highlighted the need for 'clarity, consistency, accountability and transparency' in any approach to the regulation of harmful online content.[198] The submissions identified that defining harmful online content in a clear and conclusive manner will be difficult given the many different kinds of content that can be considered harmful and the subjectivity of many of the issues.[199]

While the majority of the submissions favoured a complaints-based approach to the regulation of harmful online content whereby a victim would have access to a direct complaint mechanism available through a regulatory authority to facilitate the removal of harmful material, alternative mechanisms were also identified. For example, the potential for systemic solutions focused on online safety duties or principles and oversight by the regulator of these measures, including compliance assessments.[200] The majority of submissions made indicated a preference for a single regulatory structure, a Media Commission, with responsibility for a wide range of functions including the regulation of online harmful content and the regulation of audio-visual media services and broadcasting. [201] The majority of submissions identified potential sanction powers that could be provided to a regulator which included the power to apply administrative financial sanctions to non-compliant online services (subject to confirmation by a court) and/or the power to seek that a criminal proceeding is brought against a non-compliant online service.[202] Two main options proposed for funding a regulator were direct funding from the State or industry levies.[203]

Overall, these submissions informed the drafting process of the General Scheme of the OSMRB and influenced the form and structure of the Media Commission.

4.5.1.2 Policy Papers

Following the consultation period, the Department of Communications, Climate Action and Environment engaged in an intensive period of legal and policy analysis, exploring options for regulation.[204] The Department _of Communications, Climate Action and Environment prepared an extensive series of policy papers to 'inform decision making

[198] ibid 21.
[199] ibid.
[200] ibid 22.
[201] ibid 34.
[202] ibid 41.
[203] ibid 36.
[204] Government of Ireland, Online Safety and Media Regulation Bill, Summary of the virtual workshop on the regulatory framework for online safety (18 June 2020).

on the approach to drafting' the general scheme of the proposed OSMRB. Eight policy papers were prepared by the Government, as follows:

1.Regulatory structures and functions paper 1

2.Regulatory structures and functions paper 2

3.Regulatory powers and sanctions

4.Defining harmful online content

5.Approach to the regulation of harmful online content

6.Services in scope of the regulatory framework for online safety

7.Approach to funding regulation

8.Approach to the regulation of audiovisual media services [205]

The recommendations made in these papers were informed by legal advice, technical policy analysis and stakeholder consultation and form 'the bulk' of the general scheme of the proposed Bill.[206]

4.5.1.3 Ongoing engagement

In addition to the public consultation and policy papers, the Department of Communications, Climate Action and Environment has and continues to engage with relevant stakeholders on a 'bilateral basis'.[207] Relevant stakeholders include the National Advisory Council for Online Safety, the Department of Justice and Equality, the Broadcasting Authority of Ireland, the Data Protection Commission, An Garda Síochána, the European Commission, Children's Rights Alliance, Technology Ireland, the Irish Council for Civil Liberties, Carnegie Trust UK, Global Partners Digital, and many academics.[208]

[205] Government of Ireland, Online Safety and Media Regulation Bill, Annex to the Regulatory Impact Analysis.
[206] Government of Ireland, Online Safety and Media Regulation Bill, Summary of the virtual workshop on the regulatory framework for online safety (18 June 2020); Government of Ireland, Online Safety and Media Regulation Bill, Annex to the Regulatory Impact Analysis.
[207] Government of Ireland, Online Safety and Media Regulation Bill, Annex to the Regulatory Impact Analysis 12,13.
[208] ibid.

4.5.2 Overview of the General Scheme of the Online Safety and Media Regulation Bill 2019– The Media Commission

The General Scheme of the Bill was approved by the Government in November 2020 and subsequently published in December by Catherine Martin, the Minister for Tourism, Culture, Arts, Gaeltacht, Sport and Media.[209] The General Scheme consists of three general themes as follows:

- Parts 2 and 3: The establishment of the Media Commission and dissolution of the Broadcasting Authority of Ireland;
- Part 4: Online Safety; and
- Parts 5 and 6: On-Demand Audiovisual Services and miscellaneous provisions regarding the transposition of the EU Audiovisual Media Services Directive.

In short, the General Scheme of the OSMRB proposes three key actions. It creates a new regulator, a multi-person Media Commission, which would replace the Broadcasting Authority of Ireland.[210] It creates a regulatory framework for online safety to tackle the spread and amplification of certain defined categories of harmful online content, to be overseen by an OSC as part of the wider Media Commission.[211] Finally it updates the law for how television broadcasting services and video on-demand services, for example the RTÉ Player and Netflix type services, are regulated.[212] For the purposes of this thesis, the first two actions (in particular as covered by Parts 2, 3, and 4 of the general scheme) are of particular relevance in the context of IBSA and therefore are focused upon in the discussions below.

4.5.2.1 The Media Commission: structure, funding, and objectives

Structure

A key action under the General Scheme of the OSMRB is the establishment of a Media Commission. Head 41 of the General Scheme sets out that the Broadcasting Authority of

[209] Houses of the Oireachtas, 'Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht seeks stakeholder and expert submissions on Online Safety and Media Regulation Bill 2020' (11 February 2021) < https://www.oireachtas.ie/en/press-centre/press-releases/20210211-joint-committee-on-media-tourism-arts-culture-sport-and-the-gaeltacht-seeks-stakeholder-and-expert-submissions-on-online-safety-and-media-regulation-bill-2020/ > accessed 22 February 2022.
[210] General Scheme of the Online Safety and Media Regulation Bill, part 2 & part 3.
[211] ibid part 4.
[212] ibid part 5 & part 6.

Ireland and its Statutory Committees will be dissolved and replaced by a multi-person Media Commission with an overall focus on content regulation. The new Commission will be headed by an executive chairperson who will have overall responsibility for the management of the organisation including financial management, human resources and corporate governance. The executive chair will also be responsible for reporting to the Oireachtas Public Accounts Committee as required.[213] In addition to the executive chairperson, Head 19 sets out that a number of Commissioners will be appointed, an Online Safety Commissioner, Broadcasting Commissioner, and an On-Demand Audio-visual Services Commissioner.[214] Further Commissioners may be appointed up to a maximum of 6 which will allow the Media Commission to react and adapt to the ever-changing online environment.[215] The Media Commission will delegate relevant functions to each Commissioner however the power to seek the imposition of sanctions relating to various functions will be reserved to the Media Commission as a whole and not to individual Commissioners. [216] Justification was provided for this choice of regulatory model stating:

> Single commissioner and multi-person commissions can use specialist knowledge and experience to ensure speed and agility in decision-making and to be more responsive to sectoral developments, particularly in fast changing environments where innovation is the norm. A further advantage of a commissioner-led structure may be one of greater public visibility and public perception of a "champion" in the matters under regulation. In addition this model is the predominant one that has been used to establish regulatory bodies in recent years, for example in the Data Protection Commission, the Competition and Consumer Protection Commission and the soon to be established Corporate Enforcement Agency.[217]

---

[213] ibid Head 26.

[214] General Scheme of the Online Safety and Media Regulation Bill, Head 19 - Membership of the Commission

1. The membership of the Commission shall consist of –(a) a chairperson and such number of other whole-time members, not being less than 3 nor more than 6, as the Minister determines and appoints. 3. Each member of the Commission shall be known as a Member of the Media Commission (In this Act referred to as a "Commissioner".) 4. A Commissioner shall be appointed by the [Government/Minister] on the recommendation of the Public Appointments Service and the appointment shall be for a period of not more than 5 years from the date of his or her appointment. Explanatory note: A provision which sets the maximum number of Commissioners at 6 members and to address related matters pertaining to the appointment and removal of Commissioners. Based on section 12 of the Competition and Consumer Protection Act, 2014.

[215] Government of Ireland, Online Safety and Media Regulation Bill, Annex to the Regulatory Impact Analysis; Government of Ireland, General Scheme of the Online Safety and Media Regulation Bill Q&A, 8. 'It is desirable to have a structure in place that incorporates maximum flexibility to take account of the increasing pace of change in the regulatory landscape going forward and one in which decisions can be made in a timely and effective manner.'

[216] Government of Ireland, Online Safety and Media Regulation Bill, Summary of the virtual workshop on the regulatory framework for online safety (18 June 2020) 28, 29.

[217] Government of Ireland, Online Safety and Media Regulation Bill, Annex to the Regulatory Impact Analysis, Annex 1 - Policy paper 1 on regulatory structures and function; OECD, 'Making Reform Happen: Lessons from OECD' (OECD, May 2010) 'The great majority of independent regulators

Tríona Quill from the Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media explained that the new Media Commissioner is expected to have a level of staffing similar to the office of the Data Protection Commissioner which would amount to approximately 180 staff members which can be appointed by the Commission.[218] Staff of the current Broadcasting Authority of Ireland will be transferred to the employment of the Commission.[219]

Funding

Head 40 of the General Scheme grants the Media Commission the power to impose on regulated entities levies to provide for the cost of exercising the Commission's functions.[220] The industry levy paid by broadcasters in television and radio to the Broadcasting Authority of Ireland is proposed to instead be paid to the Media Commission.[221] Furthermore, video on-demand services and designated online services will also be subject to industry levies under the General Scheme.[222] More recently, Minister Martin announced that the broadcasting functions of the Media Commission is proposed to be part-funded, up to a maximum of 50%, from television licence receipts also.[223]

Minister Martin stated:

> 'The use of industry levies is a common approach among regulators in Ireland and will help to ensure the independence of the Media Commission. Furthermore, it is essential that the funding model is adaptable. Crucially, the proposed model will allow the Regulator to amend the levy and respond to changing circumstances.'[224]

---

in OECD countries have a multi member board or commission structure, and that this model is considered more reliable for decision making as collegiality is expected to ensure a greater level of independence and integrity'.

[218] Colm Keena, 'Staffing levels in new Media Commission expected to be similar to DPC office Office' *The Irish Times* (Dublin, 13 April 2021); General Scheme of the Online Safety and Media Regulation Bill, Head 23.

[219] General Scheme of the Online Safety and Media Regulation Bill, Head 43.

[220] ibid Head 40.

[221] ibid.

[222] ibid.

[223] Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media, 'Online Safety and Media Regulation Bill – Minister Catherine Martin proposes additional measures to assist community broadcasters, public service media and the radio sector' (Press release, 18 May 2021).

[224] Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media, 'Minister Martin presents additions to new law proposed for online safety and media regulation' (Press Release, 9 December 2020).

Objectives

Overall, one of the main objectives of the Media Commission — and of most relevance in the context of this thesis — is to administer a regulatory framework around the regulation of harmful content across the mediums of broadcasting, online, and on-demand services. It aims to minimise the availability of such content in a way that is 'effective, appropriate and legally sound'.[225] The Media Commission aims to achieve this objective while respecting EU law, the Irish legal and constitutional framework and minimising the possibility of unintended consequences such as freedom of expression violations.[226]

Head 9 of the General Scheme sets out the proposed objectives of the Media Commissioner and provide for a 'high level statement of the purpose'[227] of the Media Commission as follows:

> The Commission has the following objectives:
> 1. Ensure that democratic values enshrined in the Constitution, especially those relating to rightful liberty of expression are upheld.
> 2. Ensure that the number and categories of public service media made available in the State serve the needs of the people of the island of Ireland, having regard to the following:
> (a) linguistic, religious, ethical and cultural diversity
> (b) accessibility of services to people with disabilities
> 3. Subject to the provisions of this Act, ensure that appropriate regulatory arrangements and systems are in place to address, where appropriate, illegal and harmful online, sound and audio-visual content.
> 4. Protect the interests of children taking into account the vulnerability of children to harmful content and undue commercial exploitation.
> 5. Provide a regulatory framework that takes account of the rapidly changing technological environment and that provides for rules to be applied in a proportionate, consistent and fair manner across all services regulated, having regard to the differing nature of those services.[228]

4.5.2.2 Overview of the Media Commission: functions and core powers in the context of IBSA

The Media Commission is proposed to have many wide-ranging functions from educative and awareness raising functions to statutory powers including the ability to conduct investigations, issue compliance and warning notices and to seek the imposition of sanctions from the courts. This section will briefly outline the general functions of the

[225] Government of Ireland, Regulatory Impact Assessment, Online Safety and Media Regulation Bill (November 2020) 25.
[226] ibid.
[227] Online Safety and Media Regulation Bill 2019, Head 9 explanatory note.
[228] ibid Head 9.

Media Commission that have relevance to IBSA and after will explain the core powers of the Media Commission which have potential impact on IBSA.

Part 2 Head 10 of the General Scheme sets out the 29 functions of the Media Commission. The explanatory note to this section also sets out that the Media Commission will formally delegate functions to Commissioners and staff as appropriate.[229] As a result, individual Commissioners will take responsibility for clearly delegated functions which is particularly relevant in the case of the OSC.[230] However, as per subsection xxviii, the Media Commission may not delegate the power to impose sanctions to Commissioners or staff. Below are the relevant parts of Head 10 which have relevance in the context of IBSA. Some of these functions will be further explained in detail in the context of the OSC in section 4.4.3.

> Head 10 - Functions
> To provide that:
> (1) The Commission has the following functions:
> (v) Promote and protect the interests of the public in relation to audio-visual, audio and online content;
> (vii) To carry out an investigation, either on its own initiative or in response to a complaint made to it by any person, into any suspected breach of the relevant statutory provisions;
> (ix) To encourage compliance with the relevant statutory provisions, which may include the publication of notices containing practical guidance as to how those provisions may be complied with;
> (x) The Commission shall prepare or make codes and rules to be observed by entities operating in the following categories: (a) Audiovisual media services (b) Sound media services (c) designated online services
> (xi) The Commission shall establish or facilitate, where appropriate, a complaints mechanism or mechanisms covering some or all of the following categories:
> (a) Audiovisual media services
> (b) sound media services
> (c) designated online services
> (xiii) To promote public awareness, encourage research and conduct public information campaigns for the purpose of educating and providing information to the public in relation to:
> (a) online safety;
> (b) media literacy;
> (xiv) Promote educational initiatives and activities relating to online safety and advise, when requested, the Minister or any other Minister of the Government, Departments of State or any public body whose activities are concerned with matters relating to any of the purposes of this Act, and any educational or training institution;

[229] ibid Head 10 explanatory note.
[230] ibid Head 10 (2).

(xix) Co-operate with other authorities whether in the State or elsewhere charged with responsibility for the enforcement of laws relating to

(i) harmful online content;

(ii) the protection of children;

(iii) the allocation for the frequency range dedicated to sound and television broadcasting;

(xx) The Commission shall have a statutory role in relation to the following:

(a) reviewing existing online safety and media service related legislation and proposals for such legislation

(b) Undertaking a strategic review or reviews of the regulated sectors covering one or more of the following areas:

(I) sectoral funding

(II) technological and societal change

(III) the protection of children

(IV) other relevant strategic areas as directed by the Minister

(xxviii) Notwithstanding subsection (xxvii), the Commission may not delegate the performance of the following functions:

(a) imposition of sanctions under Head 55 (Online Safety), Head 61 (On Demand), and [Part 5 of the current Act which relates to sanctions for broadcasters]

(2) (a) The Minister may, after consulting with the Commission and any other Minister of the Government who, in the Minister's opinion, is concerned, by order confer on the Commission such additional functions relating to

(i) the regulation of audiovisual media services, the regulation of sound media services, the regulation of designated services and the protection of minors, and connected with the functions conferred on it by [insert reference to section on functions already assigned under the Act] or any order made under this [section/subsection],

(ii) the implementation of any directive or regulation of the European Union concerning [audiovisual media services, online safety, digital services, the protection of minors], and

(iii) make such provisions as the Minister considers necessary or expedient in relation to matters ancillary to or arising out of the conferral of additional functions on the Commission.[231]

In order to execute these functions, Head 11 of the General Scheme grants the Media Commission core powers including the power to create and implement codes of practice, issue compliance and warning notices, and seek the imposition of sanctions. These powers can be conferred onto specific Commissioners such as the OSC except for the imposition of sanctions which must be carried out by the Media Commission as a whole. In order to avoid repetition, these core powers will be explained in further detail in the context of the OSC in section 4.4.3.1 in the context of IBSA. Head 11 states:

[231] General Scheme of the Online Safety and Media Regulation Bill, Head 10.

> The Commission shall have all such powers as are necessary or expedient for the performance of its functions. Said powers shall include, but are not limited to; 1.the power to issue notices and warnings, 2.the power to devise, implement, monitor and review codes, including codes of practice, 3.the power to conduct investigations and inquiries, and for the necessary powers to be conferred on the Commission to conduct such investigations and inquiries, 4.the power to appoint authorised officers to carry out investigations and to confer such authorised officers such powers as are necessary to fulfil their duties,5.the power to impose administrative financial sanctions, subject to court confirmation, and the power to enter into settlement arrangements, 6.the power to prosecute summary offences[232]

The Media Commission's aim of regulating illegal and harmful content on broadcasting, online and on-demand media platforms will be supported by its powers of creating and implementing codes of practice, issuing compliance and warning notices and seeking the imposition of sanctions for non-compliance. The Media Commission can confer these powers (apart from the imposition of sanctions) to the three Commissioners who will sit within the Media Commission including the OSC.

4.5.3 Overview of the proposed Online Safety Commissioner

The 'spread and amplification' of illegal and harmful online content has increasingly become a major problem for Ireland.[233] Head 49A of the General Scheme of the Bill defines harmful online content as including:

> (a) material which it is an criminal offence to disseminate under Irish [or Union law],
> (b) material which is likely to have the effect of intimidating, threatening, humiliating or persecuting a person to which it pertains and which a reasonable person would conclude was the intention of its dissemination,
> (c) material which is likely to encourage or promote eating disorders and which a reasonable person would conclude was the intention of its dissemination, and,
> (d) material which is likely to encourage or promote [self-harm or suicide] or provides instructions on how to do so and which a reasonable person would conclude was: (i) the intention of its dissemination and (ii) that the intention of its dissemination was not to form part of philosophical, medical and political discourse.
> but does not include –
> (a)material [containing or comprising] a defamatory statement,

[232] ibid Head 11.
[233] Government of Ireland, Regulatory Impact Assessment, Online Safety and Media Regulation Bill (November 2020) 8.

(b)material that violates [data protection or privacy law],
(c)material that violates [consumer protection law], and
(d)material that violates [copyright law][234]

This definition of harmful online content is not proposed to define harmful online content as a 'singular concept' but rather it is proposed to 'enumerate definitions of categories' of material that are considered to be harmful online content.[235] While IBSA is not specifically mentioned as a category of material which is considered harmful, IBSA does fall with subsection (a) of the definition since IBSA was criminalised in 2020 under the Harassment, Harmful Communications and Related Offences Act as discussed in section 4.3.

Where not covered by existing laws, the regulation of harmful online content has been left to online services to self-regulate.[236] We have seen how reliance on self-regulation has failed to prevent the distribution of IBSA and to protect its victims. To address this issue the Government has passed targeted legislation criminalising IBSA and has committed to establishing a regulatory framework for online safety including the establishment of an OSC.[237] As stated by Minister Bruton on the 4th of March 2019, a key reason for the proposed legislation is to establish an OSC to 'oversee the regulatory framework for online safety proposed by the Bill'.[238]

The General Scheme of the OSMRB proposes the appointment of an OSC as part of a wider Media Commission to oversee the new regulatory framework for online safety. While the General Scheme does not set out the functions and powers of the OSC specifically,[239] supporting documentation explains that part 4 of the Bill which governs online safety will be carried out by an OSC. Therefore, the following sections will explain the proposed functions that will potentially be delegated to the OSC by the Media Commissioner.

The aim of the regulatory framework for online safety is to tackle the spread and amplification of certain defined categories of harmful online content[240] by creating a

[234] General Scheme of the Online Safety and Media Regulation Bill, Head 49A.
[235] ibid Head 49A explanatory note.
[236] Government of Ireland, Regulatory Impact Assessment, Online Safety and Media Regulation Bill (November 2020) 8.
[237] ibid.
[238] Government of Ireland, General Scheme of the Online Safety and Media Regulation Bill Q&A.
[239] General Scheme of the Online Safety and Media Regulation Bill, Head 10 allows the Media Commissioner to delegate functions to the OSC.
[240] General Scheme of the Online Safety and Media Regulation Bill, Head 49A
"harmful online content" includes –
(a) material which it is an criminal offence to disseminate under Irish [or Union law],

system of effective oversight. This system will centre around the creation and implementation of online safety codes.[241] The OSC will also have a number of compliance and enforcement powers, including the powers to require reporting, initiate investigations and audits,[242] issue compliance and warning notices,[243] and sanction non-compliant online services through the Media Commission.[244] The purpose of this approach is to create 'a cycle of harm minimisation', whereby fewer people will be exposed to harmful online content over time.[245] The regulatory framework will also incorporate the regulation of video sharing platform services required by the revised Audiovisual Media Services Directive.[246] Head 56 of the General Scheme outlines which services fall under the Media Commission's regulatory powers (which will potentially be delegated to an OSC). This provision enables the Media Commission/OSC to 'designate online services' to be subject to robust regulation. The OSC under the Media Commission will have the power to 'designate individual and categories of online services from a wider pool of relevant online services[247] to abide by any online safety codes the Commission deems necessary'. [248] This section further provides that 'video sharing

(b) material which is likely to have the effect of intimidating, threatening, humiliating or persecuting a person to which it pertains and which a reasonable person would conclude was the intention of its dissemination,
(c) material which is likely to encourage or promote eating disorders and which a reasonable person would conclude was the intention of its dissemination, and,
(d) material which is likely to encourage or promote [self-harm or suicide] or provides instructions on how to do so and which a reasonable person would conclude was: (i) the intention of its dissemination and (ii) that the intention of its dissemination was not to form part of philosophical, medical and political discourse.
but does not include –
(a) material [containing or comprising] a defamatory statement,
(b) material that violates [data protection or privacy law],
(c) material that violates [consumer protection law], and
(d) material that violates [copyright law]
The explanatory note of Head 49A explains that this is not a definition of harmful content but rather 'enumerates descriptions of categories of material that are considered to be harmful online content'. Part 4 Head 49B grants the Media Commission the ability to propose to include or exclude further categories of material from the definition of harmful online content.

[241] Government of Ireland, Online Safety and Media Regulation Bill, Summary of the virtual workshop on the regulatory framework for online safety (18 June 2020) 4, 5.

[242] General Scheme of the Online Safety and Media Regulation Bill, Head 50B.

[243] ibid Head 53.

[244] ibid Head 16A & Head 54A.

[245] Government of Ireland, Online Safety and Media Regulation Bill, Summary of the virtual workshop on the regulatory framework for online safety (18 June 2020) 4, 5.

[246] ibid.

[247] General Scheme of the Online Safety and Media Regulation Bill, Head 2 defines relevant online service as: "relevant online service" means an information society service established in the State that [facilitates the dissemination of or access to] user-generated content via an electronic communications network; [refers to the definition of information society service from the eCommerce Directive 2000 (Directive 2000/31/EC) and a definition of user-generated content, which is adapted from the definition of user-generated video in the revised Audiovisual Media Services Directive (Directive (EU) 2018/1808)].

[248] General Scheme of the Online Safety and Media Regulation Bill, Head 56.

platform services[249] are a category of designated online services'. However, audiovisual media services[250] are exempt from being designated.[251] Therefore, the OSC can designate any online service or categories of online services that allow users to share, spread or access content that other users have made available.[252] As a result, a wide range of services may fall into the scope for potential designation. However, this does not imply that such services should or will be designated.[253] The types of services which may fall under the scope includes:

> Social media services, Public boards and forums, Online gaming services, Ecommerce services, where they facilitates the dissemination of or access to user-generated content, Private communication services, Private online (cloud) storage services, Press publications, where they facilitate the dissemination of or access to user-generated content, Online search engines, and, Internet service providers.[254]

4.5.3.1 Core Powers of the Online Safety Commissioner in the context of IBSA

It is proposed that the Media Commission will delegate 6 key powers to the OSC to use to combat the availability of harmful online content such as IBSA.

The Media Commission's/OSC's key powers which will be discussed in more detail below are:

1. The creation and implementation of online safety codes
2. The creation of guidance materials
3. The auditing of complaint handling systems and mechanisms

---

[249] General Scheme of the Online Safety and Media Regulation Bill, Head 2 defines video sharing platform services as: "video-sharing platform service" means a media service where the principal purpose of the service or of a dissociable section thereof or an essential functionality of the service is devoted to providing programmes, user-generated videos, or both, to the general public, for which the video-sharing platform provider does not have editorial responsibility, in order to inform, entertain or educate, by means of an electronic communications network and the organisation of which is determined by the video-sharing platform provider, including by automatic means or algorithms in particular by displaying, tagging and sequencing." [adapted from the definition of video sharing platform service in the revised Audiovisual Media Services Directive (Directive (EU) 2018/1808)]

[250] General Scheme of the Online Safety and Media Regulation Bill, Head 2 defines audiovisual media service as: "audiovisual media service" means (a) a media service which is under the editorial responsibility of a media service provider and the principal purpose of which is the provision of programmes in order to inform, entertain or educate, to the general public by electronic communications networks, and is either an audiovisual broadcasting service or an on-demand audiovisual media service, or (b) an audiovisual commercial communication; [adapted from the definition of audiovisual media service in the revised Audiovisual Media Services Directive (Directive (EU) 2018/1808)].

[251] General Scheme of the Online Safety and Media Regulation Bill, Head 56.

[252] ibid Head 56 explanatory note.

[253] ibid.

[254] General Scheme of the Online Safety and Media Regulation Bill, Head 56 explanatory note; Government of Ireland, Online Safety and Media Regulation Bill, Summary of the virtual workshop on the regulatory framework for online safety (18 June 2020) 23.

4. The administering of a systemic complaint scheme
5. The issue of compliance and warning notices
6. The imposition of sanctions (reserved only for the Media Commission)

1. The creation and implementation of online safety codes

The proposed OSC's regulatory framework is based around the creation and implementation of safety codes. Head 50A provides that the Media Commission (or assuming delegation, the OSC) shall prepare online safety codes, which may be revised at any stage, governing standards and practices that shall be observed by designated online services.[255] The online safety codes are proposed to include areas such as measures for online services to take to tackle the availability of harmful online content on their services, user complaint and/or issues handling mechanisms operated by online services, and risk and impact assessments for online services to take in relation to the availability of harmful online content on their services.[256] Head 50A also provides a list of matters that the Media Commission shall have regard to in preparing online safety codes, including matters relating to EU law, the nature and scale of services, transparency and fundamental rights.[257] The General Scheme of the Bill provides that designated online services are obliged to comply with the online safety codes.

In short, it will be the responsibility of the Media Commission (or assuming delegation, the OSC) to develop 'high level principle-based codes governing standards and practices'[258] upon which designated online services are then required to develop measures to meet the principles set out in the high-level codes. The Media Commission/OSC can then assess whether these measures are working in practice through information requests, investigations and audits. [259] This is a systemic approach to regulation where the emphasis is on the online environment as opposed to individual instances of harm.

Head 50B provides that the Media Commission (or assuming delegation, the OSC) has the power to request information from designated online services in relation to their compliance with any online safety code and that it is an offence for a designated online

[255] General Scheme of the Online Safety and Media Regulation Bill, Head 50A (1).
[256] General Scheme of the Online Safety and Media Regulation Bill Head 50 (2); Government of Ireland, General Scheme of the Online Safety and Media Regulation Bill Q&A.
[257] General Scheme of the Online Safety and Media Regulation Bill, Head 50A (3).
[258] General Scheme of the Online Safety and Media Regulation Bill, Head 50A explanatory note.
[259] ibid Head 50B explanatory note.

service not to comply with such a request.[260] Furthermore the Media Commission/OSC may examine the compliance of designated online services to the safety codes and may appoint authorised officers to carry out these investigations.[261] Following an investigation, the Media Commission/OSC may issue a compliance notice (explained later in this section) to the designated online service mandating the service to take specific steps to improve their compliance with the safety codes. It is proposed that these powers to request information, conduct investigations, and issue compliance notices will allow the Media Commission/OSC to see if the actions taken by an online service in order to comply with the online safety codes are 'robust and if they actually work in practice'.[262]

2. The creation of guidance materials

In addition to binding online safety codes, the Media Commission/OSC may also make non-binding online safety guidance materials, enabling the Media Commission to elaborate on matters addressed through codes and to test regulatory approaches prior to making them binding through codes.[263] Head 51A provides that the Media Commission (or assuming delegation, the OSC) may issue guidance materials relating to harmful online content and age inappropriate online content.[264] Relevant online services and designated online services must have regard to these guidance materials. Unlike the safety codes, however, the guidance materials will be non-binding.[265] The guidance materials are proposed to allow the Media Commission to 'elaborate' on matters addressed through codes and to 'test regulatory approaches' prior to making them binding through codes.[266] As a result, some approaches outlined in the guidance materials, if proved to be successful may transition to becoming a safety code and would be then binding.[267]

3. The auditing of complaint handling systems and mechanisms

---

[260] ibid Head 50B.
[261] General Scheme of the Online Safety and Media Regulation Bill, Head 50B (5).
[262] Government of Ireland, General Scheme of the Online Safety and Media Regulation Bill Q&A.
[263] Government of Ireland, Online Safety and Media Regulation Bill, Summary of the virtual workshop on the regulatory framework for online safety (18 June 2020) 17.
[264] General Scheme of the Online Safety and Media Regulation Bill, Head 51A (1); Head 49C defines - "age inappropriate online content" means material which may be unsuitable for exposure to minors and that they should not normally see or hear and which may impair their development, taking into account the best interests of minors, their evolving capacities and their full array of rights, and includes: (a)material containing or comprising gross or gratuitous violence, (b)material containing or comprising cruelty, including mutilation and torture, towards humans or animals, and, (c)material containing or comprising pornography.
[265] General Scheme of the Online Safety and Media Regulation Bill, Head 51A (2).
[266] Government of Ireland, Online Safety and Media Regulation Bill, Summary of the virtual workshop on the regulatory framework for online safety (18 June 2020).
[267] ibid.

The Media Commission (or assuming delegation, the OSC) will also have the power to audit any user complaints and issues handling systems operated by designated online services.[268] Following an audit the Media Commission/OSC may issue a compliance notice to direct a designated online service to take specified actions, including to remove or restore individual pieces of content and to make changes to the operation of their systems. [269]

4. The administering of a systemic complaint scheme

The General Scheme of the Bill also provides that the Media Commission (or assuming delegation, the OSC) will create a 'systemic complaint scheme'/ 'super complaints scheme'[270] whereby 'nominated bodies' such as 'expert charities' will be able to highlight systemic issues with relevant online services and designated online services to the Media Commission/OSC. Head 52B outlines that the Media Commission (or assuming delegation, the OSC) will receive notices from nominated bodies and have a timeline upon which to respond to notices.[271] However the practical functioning of this scheme has yet to be outlined.[272] Details which will need to be outlined by the Media Commission following establishment include 'the form in which it will receive notices, the timeline in which it will respond to notices, the criteria for nomination, the process through which a body can apply for nomination, the process through which a body's nominated status can be revoked by the Media Commission, and, the criteria for revocation of a body's nominated status.'[273] Upon receiving a notice, the Media Commission (or assuming delegation, the OSC) may conduct an investigation in accordance with Head 50B to examine whether the designated online service is in compliance with the safety codes.[274] If the service is not already designated, the Media Commission/OSC may consider designating a relevant online service in accordance with Head 56 so to make the online safety codes binding upon that service.[275] Upon conducting an investigation, the Media Commission (or if delegated, the OSC) may issue a compliance notice where necessary.

---

[268] General Scheme of the Online Safety and Media Regulation Bill, Head 52A (1).
[269] ibid Head 52A (2).
[270] General Scheme of the Online Safety and Media Regulation Bill, Head 52B explanatory note 'This provision provides the Media Commission with the power to devise and operate a so called "super complaints". This is where nominated bodies, for example expert NGOs or members of the European Regulators Group for Audiovisual Media Services, would have a channel to bring issues they have identified with a relevant or designated online service to the Commission's attention'.
[271] General Scheme of the Online Safety and Media Regulation Bill, Head 52B (2).
[272] ibid Head 52B (2).
[273] ibid Head 52B (3).
[274] ibid Head 52B (5).
[275] ibid Head 52B (6).

This mechanism does not provide for an examination of individual complaints but relies on a systemic issue being identified by nominated bodies – potentially on the basis of individual complaints brought to them indicating a broader problem.[276]

5. Power to oblige the consideration of mediation

Head 52C (1) of the General Scheme of the Bill provides that where there is a dispute between a designated online service and a user, or group of users 'both parties shall consider mediation[277] as a method of reaching a mutually acceptable agreement to resolve the dispute'.[278] The Media Commission (or assuming delegation, the OSC) may investigate the compliance of a designated online service with online safety codes on the basis of information relating to any dispute and initiate an audit if necessary.[279] This provision does not prevent the highlighting of an issue with a designated service's reporting mechanism or compliance with safety codes through the systemic complaints system.[280] The explanatory notes accompanying Head 52C explains that the costs of mediation may be 'borne by one or both parties, or another party, as agreed by the parties to the dispute'.[281]

6. The issue of compliance and warning notices

Head 53 of the General Scheme provides for the procedure by which the Media Commission (or assuming delegation, the OSC) may issue compliance and warning notices to a designated online service.

The Media Commission (or assuming delegation, the OSC) may issue compliance notices if it is of the view that a designated online service is not in compliance with an online safety code, following issues discovered during an audit or investigation, or following a complaint made via the systemic complaints scheme.[282]

A compliance notice will outline the Commission's views and how it formed those views. It will outline the steps the Media Commission/OSC deems necessary for the designated online service to take to bring itself into compliance which may include changing a

[276] Government of Ireland, Regulatory Impact Assessment, Online Safety and Media Regulation Bill (November 2020) Policy Paper 5, 26.
[277] General Scheme of the Online Safety and Media Regulation Bill, Head 52(5) "mediation" means a facilitative and voluntary process in which parties to a dispute, with the assistance of a mediator, attempt to reach a mutually acceptable agreement to resolve the dispute.
[278] General Scheme of the Online Safety and Media Regulation Bill, Head 52C (1).
[279] ibid Head 52 C (3) (4).
[280] ibid Head 52 C (2).
[281] ibid Head 52 C explanatory note.
[282] ibid Head 53 (1).

system or policy, or the removal or restoration of content, and the timescale in which those steps must be taken.[283] If the steps to be specified in a compliance notice are about the removal or restoration of material the Commission may invite submissions from the uploader and complainant before it issues the notice.[284]

If following the issue of a compliance notice, the designated online service does not comply and does not provide a reasonable explanation to the Media Commission/OSC for its non-compliance, or it does not provide a satisfactory plan to bring itself into compliance the Commission may issue a warning notice.[285]

A warning notice represents an 'escalation of intervention' by the Media Commission/OSC regarding non-compliance by a designated online service.[286] A warning notice will outline the view of the Media Commission/OSC regarding the alleged non-compliance[287] and the steps which the Commissioner deems necessary for the designated online service to take to bring itself into compliance, within a specified time frame.[288] The warning notice will also outline the actions which will be taken if the designated online service does not bring itself into compliance.[289]

A designated online service that does not comply with the steps outlined in a warning notice issued to it by the Media Commission/OSC shall be guilty of an offence[290] and may be subject to a sanction under Head 54[291] as outlined in the next section.

7. The imposition of sanctions

Non-compliance with a warning notice will be an offence under the General Scheme of the Bill and the Media Commission may seek to apply a civil sanction. Head 54A provides for the range of sanctions available to the Media Commission including administrative financial sanctions,[292] orders compelling compliance, or the blocking of access to the

[283] ibid Head 53 (2) (3).
[284] ibid.
[285] General Scheme of the Online Safety and Media Regulation Bill, Head 53 (4); Government of Ireland, Online Safety and Media Regulation Bill, Summary of the virtual workshop on the regulatory framework for online safety (18 June 2020).
[286] Government of Ireland, Online Safety and Media Regulation Bill, Summary of the virtual workshop on the regulatory framework for online safety (18 June 2020).
[287] General Scheme of the Online Safety and Media Regulation Bill, Head 53 (5).
[288] ibid Head 53 (6).
[289] General Scheme of the Online Safety and Media Regulation Bill, Head 53 (6); Government of Ireland, Online Safety and Media Regulation Bill, Summary of the virtual workshop on the regulatory framework for online safety (18 June 2020).
[290] General Scheme of the Online Safety and Media Regulation Bill, Head 53 (11).
[291] ibid Head 53 (12).
[292] Government of Ireland, Online Safety and Media Regulation Bill, Summary of the virtual workshop on the regulatory framework for online safety (18 June 2020). 'In deciding whether to impose an administrative

designated online service in Ireland.[293] The Media Commission must apply to the court to apply these sanctions whereby the designated online service in question will have the opportunity to dispute its application. Head 54 provides the Media Commission with the discretion to determine the sanction it may seek having regard to the nature of the non-compliance of the designated online service.[294]

4.5.4 The regulation of IBSA by the Media Commission/OSC

The focus of the proposed regulatory framework for online safety is to regulate online services rather than the behaviour of individuals.[295] The Government confirmed that where an instance of harmful online content is criminal in nature, it will continue to be a matter for An Garda Síochána to investigate such instances.[296] Therefore victims of IBSA will not be able to directly seek a remedy from the Media Commission/OSC but rather must still seek a remedy by bringing their case to An Garda Síochána and seek a criminal prosecution. While a victim can raise a matter relating to a service provider's systemic processes or lack of compliance with safety codes to a nominated body who may then pass the matter to the Media Commission/OSC if it is believed to be indicative of a systemic issue, a victim cannot make a complaint directly to the Media Commission/OSC about a specific piece of content such as an intimate image being hosted by a platform. Moreover, the Media Commission/OSC does not have power to issue compliance or warning notices to end-users. However, the Media Commission/OSC can oblige the

financial sanction or the amount of such a sanction the Commission must consider a number of factors including: 'whether the sanction is appropriate and proportionate to the wrongdoing, whether the sanction will act as a sufficient incentive to ensure future compliance, the seriousness of the wrongdoing, and whether the designated online service can provide any excuse or explanation for the wrongdoing.' As the imposition of an administrative financial sanction may constitute the administration of justice, the Media Commission will not have the power to make a final determination to impose such sanctions unless the regulated entity asks the Commission to do so. A designated online service may appeal a decision to impose an administrative financial sanction or the amount of that sanction to either the Circuit Court or the High Court, depending on the amount of the sanction. If a designated online service does not pursue an appeal or ask the Media Commission to impose the sanction then the Commission may apply to the Circuit Court to confirm the decision.'; Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media, 'Minister Martin presents additions to new law proposed for online safety and media regulation' (Press Release 9 December 2020). 'The upper amount of the administrative financial sanctions that the Online Safety Commissioner may seek to impose on a non-compliant designated online service will be €20m or 10% of turnover, whichever is higher'.

[293] General Scheme of the Online Safety and Media Regulation Bill, Head 54.

[294] ibid Head 54 explanatory note.

[295] Government of Ireland, Online Safety and Media Regulation Bill, Summary of the virtual workshop on the regulatory framework for online safety (18 June 2020) 9.

[296] ibid.

service provider to engage in mediation with the victim for an issue they have with a reporting mechanism or issue with hosted content.

It is clear – at least from the General Scheme – that the role of the Media Commission/OSC is envisioned to be primarily focused on ensuring that online services are taking appropriate steps to provide a 'safe' online environment – which in the context of IBSA would limit the spread and amplification of intimate images on a systemic level rather than a direct line for victims of IBSA to seek help and support. Notwithstanding this, social media reporting mechanisms may become more reliable, robust and impactful as a result of the proposed safety codes. Therefore, victims may be able to regain control of their image through social media platform's more regulated complaint handling systems operated in accordance with the still to be created codes. It also appears to be the intention of the proposals that the Media Commission/OSC educative and awareness raising functions should have a positive effect in reducing the prevalence of IBSA, although due to the lack of detail concerning this aspect of this role, it is difficult to discern its likely impact.

4.6 Conclusion

This chapter mapped out the development of the Irish response to IBSA up to the introduction of the OSMR Bill and analysed this response from a victim-centred perspective. This Chapter began by providing an overview of the Irish situation in the context of IBSA prior to the more recent legislative proposals. The discussion of Irish cases – such as the case of 'Jane' and Dara Quigley – highlighted the absence of remedies for victims of IBSA in Irish law. Identified challenges that mirrored challenges found in the Australian system include issues around anonymity, jurisdiction, and law enforcement resources training. Stakeholders at the Open Policy Debate as discussed in section 4.2.6 identified issues with lack of police training and enforcement similar to Australia while the 'Dispatch Revelations' and the 'Discord Leak' discussed in sections 4.2.8 and 4.2.9 highlighted the role of intermediaries and the failure of self-regulation. While the criminalisation of IBSA was identified as a positive step for victims of IBSA in Ireland, even where the criminal process runs as intended, it only provides for the prosecution of the perpetrator. This is often a secondary priority of victims of IBSA, who often place

most value on the removal of the images from the internet.[297] Furthermore the potential of re-traumatisation of victims during criminal proceedings and lengthy court processes highlighted the need for a supplementary avenue of complaint for victims.

Next, this Chapter applied the victim-centred framework developed in prior chapters to the Irish response to IBSA prior to the enactment of the OSMRA. Following the application of the victim-centred framework, it was evident that while some victim needs were at least partially addressed, others remained completely unaddressed and there was a need for additional tools/mechanisms of redress. Having considered the landscape prior to its introduction, it was necessary to provide background insight into the development of the OSMRA. Innovations of particular note in the OSMRB were the establishment of a systemic online safety regime and the appointment of an Online Safety Commissioner to operate within a newly established statutory authority to be known as 'Coimisiún na Meán'.

Overall, this chapter highlighted the prevalence of IBSA within the Irish context and the need not only for more robust criminal legislation but also a clear supplementary avenue of redress aside from traditional criminal and civil approaches. Chapter 5 carries forward the victim-centred framework to assess the potential of Ireland's new approach to online safety to adequately address the needs of victims of IBSA.

[297] Nicola Henry, Asher Flynn & Anastasia Powell (2018) 19 Policing image-based sexual abuse: stakeholder perspectives, Police Practice and Research 565.

Chapter 5: Assessment of the Irish Online Safety Commissioner from a victim-centred perspective

5.1 Introduction

While the criminalisation of IBSA under the Harassment, Harmful Communications and Related Offences Act 2020 is a positive tool for victims and potential victims of IBSA, gaps in remedies and enforcement persist.[1]

As highlighted in Chapter 2 and Chapter 3, over a number of years Australia has introduced reporting schemes – including the IBA scheme, Cyberbullying Complaints Scheme, and Online Content Scheme – in an effort to tackle the challenge of harmful online content and to provide an avenue of redress for victims. From the research conducted in this thesis, the importance of the role of the Office of the eSafety Commissioner (OESC) and its associated structures is clear. Under the recently enacted Online Safety and Media Regulation Act 2022 (OSMRA), a new Online Safety Commissioner (OSC) was established within the structures of the newly established Media Commission.[2] Many of the crucial operative components of the OSMRA– most notably the Online Safety Codes – are yet to be drafted. The assessment in this chapter is focused on the development of the legislation which has led to this point.

Building on the context and history provided in Chapter 4, this chapter analyses the pertinent proposals addressing online safety issues originally made in the General Scheme of the Online Safety and Media Regulation Bill and the Online Safety and Media Regulation Bill (OSMRB) as initiated. This chapter will use lessons learned from the desk-based analysis of the OESC conducted in Chapter 2 and the interviews discussed in Chapter 3 in order to assess the ability of the OSC to respond to the needs of victims of IBSA. To further inform this analysis, other proposals such as those contained in the LRC Report on Harmful Communications and Digital Safety, which recommended the establishment of a Digital Safety Commissioner (DSC), will also be used to identify the merits and demerits of the OSC.

As noted in the introduction to this thesis, in 2020 Minister McEntee highlighted the

[1] Nicola Henry, Asher Flynn & Anatasia Powell, 'Policing IBSA: Stakeholders Perspectives' (2018) 19 Police Practice and Research 565.

[2] Niamh Hodnett was appointed as the OSC. Press and Information Office, 'Minister Martin Announces Forthcoming Appointment of Executive Chairperson and Commissioners in Coimisiún na Meán' <Minister Martin announces forthcoming appointment of Executive Chairperson and Commissioners in Coimisiún na Meán - MerrionStreet> accessed 17 May 2023.

importance of the adoption of a 'victim-centred approach' to sex crimes in Ireland.[3] Minister McEntee highlighted IBSA in this context and called for the prioritisation of victims and their needs. Adopting a victim-centred approach by applying the framework developed in the earlier chapters, this chapter aims to address Minister McEntee's call and provides clear recommendations on what legal reforms are needed in order to better address the needs of victims of IBSA. In particular, the powers of the OSC and the existence of reporting and enforcement mechanisms for victims of IBSA will be discussed. This chapter will analyse the powers and functions of the OSC in comparison with Australia's OESC. As the Australian Parliament has, subsequent to the conducting of the stakeholder interviews discussed in this thesis, updated the law in this area with the passage of the Online Safety Act 2021, the relevant changes are also used to assess the approach taken in Ireland. The lessons gained from studying the development of the Australian system and from interviewing expert stakeholders are of continued relevance in the Irish context, particularly due to the limited time the Online Safety Act 2021 has been in effect. Finally, this chapter outlines the updates in this area including the enactment of OSMRA 2022 and the findings of the expert committee that was formed to assess the feasibility of an individual complaints mechanism. This chapter considers the potential of the nascent regulatory system for online safety to adequately address the needs of victims of IBSA.

5.2 Assessment of the OSC as set out under the General Scheme of the Bill in the context of image-based sexual abuse

In order to assess the merits and limitations of the OSC, various documents have been analysed including part 4 of the General Scheme of the Online Safety and Media Regulation Bill, transcripts of Dáil debates and published questions and answers, pre-legislative scrutiny submissions, and the published data from a virtual workshop. The Dáil debates include input from cabinet members, government backbenchers, and opposition TDs. As part of the scrutiny of the General Scheme of the Bill, the Government invited written submissions from a range of stakeholders including experts in the areas of online safety, child protection, mental health, and media law and policy, as well as

[3] Shauna Bowers and Vivienne Clarke, 'McEntee wants to see 'victim-centred approach' to sex crimes: Action plan will be before Government within 10 weeks, says Minister for Justice' *The Irish Times* (Dublin, 7 August 2020).

regulatory bodies and representatives of civil society.[4] Due to the Covid-19 restrictions, a planned stakeholder workshop on the regulatory framework for online safety due to be held in March 2020 was postponed and subsequently held virtually on 18 June 2020.[5] The workshop engaged 60 participants from a wide range of backgrounds, including 'expert academics, representatives of commercial organisations, domestic and international NGOs, the European Commission, and public bodies.'[6] Following the analysis of these documents, 10 key points can be identified for further discussion:

1. Assessment of the definition of harmful content
2. The OSC and the need for clarity and specific provision
3. Issues with the systemic complaints system
4. Issues with the obligation for mediation
5. The need for an individual complaints mechanism
6. The merits of an intermediate goal
7. Transparency for reporting mechanisms
8. The importance of sanctions but the need for safeguards
9. Collaboration
10. The need for greater educational and awareness raising functions

5.2.1 Assessment of the definition of harmful content

The definition of harmful content under Head 49A provided descriptions of categories of material that are considered to be harmful online content. These include material which is a criminal offence to disseminate (such as IBSA under the Harassment, Harmful Communications and Related Offences Act), material which can intimidate, threaten or humiliate a person, material which promotes eating disorders, and material which promotes self-harm.[7] Head 49B further granted the Media Commission (or assuming delegation, the OSC) the ability to propose to include or exclude further categories of material from the definition of harmful online content. The decision to outline categories

[4] Houses of the Oireachtas, 'Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht seeks stakeholder and expert submissions on Online Safety and Media Regulation Bill 2020' (11 February 2021) < https://www.oireachtas.ie/en/press-centre/press-releases/20210211-joint-committee-on-media-tourism-arts-culture-sport-and-the-gaeltacht-seeks-stakeholder-and-expert-submissions-on-online-safety-and-media-regulation-bill-2020/ > accessed 22 February 2022.
[5] Government of Ireland, Online Safety and Media Regulation Bill, Summary of the virtual workshop on the regulatory framework for online safety (18 June 2020).
[6] ibid 6.
[7] General Scheme of the Online Safety and Media Regulation Bill, Head 49A.

of content rather than a singular definition was informed by the approaches taken by LRC in their Report on Harmful Communications and Digital Safety and the UK's Online Harms White Paper.

While this approach was supported by representatives of RTÉ,[8] the Children's Rights Alliance,[9] and Technology Ireland,[10] Head 49A had limitations in the context of IBSA. IBSA is a very problematic category of harmful online content, with young people being particularity vulnerable.[11] Research carried out by Women's Aid on intimate relationships found that young people in Ireland are reluctant to raise online abuse issues and are reluctant to seek support.[12] As a result it is important that IBSA is 'named and made visible'[13] in the legislation and is not 'hidden'[14] in the category of 'illegal content'.[15]

5.2.2 The OSC and the need for clarity and specific provision

One of the core intentions of the General Scheme, according to the Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media, was to provide for the: 'appointment of an OSC as part of a wider Media Commission to oversee the new regulatory framework for online safety.'[16] The Department stated that the OSC under the regulatory framework in Part 4 of the General Scheme would:

- designate online services and categories of online services for regulation

- make online safety codes and decide which codes apply to which online services

- assess the compliance of online services with online safety codes,

- audit any complaint or issues handling processes that online services operate,

---

[8] Rory Coveney, Director of Strategy RTÉ, 'Online Safety and Media Regulation Bill Opening Statement ' <2021-05-20_opening-statement-rory-coveney-director-of-strategy-rte_en (1).pdf> accessed 22 February 2022.

[9] Children's Rights Alliance, Submission to the Joint Oireachtas Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht on the General Scheme of the Online Safety and Media Regulation Bill (8 March 2021).

[10] Technology Ireland, submission on the General Scheme of the Online Safety and Media Regulation Bill (8 March 2021).

[11] Women's Aid, Submission to the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht on the General Scheme of the Online Safety and Media Regulation Bill (March 2021).

[12] Women's Aid, *One in Five Women Report, Experience Intimate Relationship Abuse Women's Aid 2020, TOO INTO you.*

[13] Women's Aid, Submission to the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht on the General Scheme of the Online Safety and Media Regulation Bill (March 2021).

[14] ibid.

[15] General Scheme Online Safety and Media Regulation Bill, Head 49A (a).

[16] Dáil Éireann Debate, 'Online Safety' (17 December 2020) < https://www.oireachtas.ie/en/debates/question/2020-12-17/319/> accessed 22 February 2022.

- operate a 'super complaints' scheme for nominated bodies such as expert charities to bring issues with online services to the Commissioner's attention.[17]

While the role and duties of the OSC were reported in documents accompanying the General Scheme, there was no specific or detailed provision in the General Scheme establishing the role of the OSC or specifying the functions of the OSC. The functions of the Media Commission in Head 10 had been described as 'overly broad and vague'[18] and lacking clarity as to the delegation of functions to appointed Commissioners and failed to provide for the role of the OSC. An explanatory note, under Head 10, states:

> It should be noted that it is intended that the Commission will formally delegate functions to Commissioners and staff as appropriate. While the delegation of functions is ultimately a matter for the Commission itself, this provision is desired from a policy perspective as the Minister wishes that individual Commissioners can take responsibility for clearly delegated functions. This is particularly relevant in the case of the OSC. [19]

This was the only express reference to the OSC in the General Scheme of the Bill, in contrast to the LRC proposed DSC which had a specific role and functions as outlined in Chapter 4 section 4.2.2.2.[20]

This lack of provision for the specific role and functions of the OSC and lack of express reference to the OSC had been described as 'concerning' by the Children's Rights Alliance, the Irish Council of Civil Liberties, the Human Rights and Equality Commission, the Ombudsman for Children, The Institute for Future Media, and Samaritans Ireland.[21] Considering that the OSC had been proposed to have a substantial

---

[17] Dáil Éireann Debate, 'Online Safety' (17 December 2020) < https://www.oireachtas.ie/en/debates/question/2020-12-17/319/> accessed 22 February 2022.

[18] Irish Council of Civil Liberties, ICCL submission on the Online Safety and Media Regulation Bill To: Oireachtas Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht Date (8 March 2021).

[19] General Scheme of the Online Safety and Media Regulation Bill General Scheme, Head 10 explanatory note.

[20] Digital Safety Commissioner Bill 2017, s 3.

[21] Children's Rights Alliance, Submission to the Joint Oireachtas Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht on the General Scheme of the Online Safety and Media Regulation Bill (8 March 2021); Irish Council of Civil Liberties, ICCL submission to Pre-legislative scrutiny of the General Scheme of the Online Safety and Media Regulation Bill, Submission to the Joint Oireachtas Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht (26 May 2021); Irish Council of Civil Liberties, ICCL submission on the Online Safety and Media Regulation Bill To: Oireachtas Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht Date (8 March 2021); Irish Human Rights and Equality Commission, Submission to the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht on the General Scheme of the Online Safety and Media Regulation Bill (March 2021); Ombudsman for Children, General Scheme of the Online Safety and Media Regulation Bill 2020, Submission by the Ombudsman for Children's Office to the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht (4 March 2021); The Institute for Future Media, Democracy and Society (FuJo) and the National Anti-Bullying Research, The General Scheme of the Online Safety and Media

impact on the rights of users and operators of online services and to have a significant role in overseeing the regulatory framework under the General Scheme,[22] this could not be viewed as a promising start. It should be made very clear how individual Commissioners, and in particular the OSC, will operate within the Commission in terms of decision making and the delegation of powers.[23]

5.2.3 Issues with the systemic complaints system and need for an individual complaints system

The systemic nature of the Irish regulatory approach can be described as 'system-oriented'[24] rather than 'person-centred'[25] as the focus of the scheme is to provide an avenue to complain about service providers' systems or lack of compliance with Online Safety Codes. The General Scheme of the OSMRB did not provide for complaints about individual pieces of harmful content. The systemic approach obliges service providers to abide by codes set out by the Media Commission/OSC in the design and operation of their services. The Media Commission/OSC would then engage in the oversight of the service providers to ensure they are meeting their obligations under the safety codes. The review of service providers complaints-handling systems provides another layer of checks in order to administer this systemic approach. The systemic approach based on safety codes and oversight of compliance by the Media Commission/OSC has been described by the Department of Communications, Climate Action and Environment as being 'more effective in improving online safety in a holistic way than an approach which focused on individual complaints'.[26] An important aspect of the systemic complaints system is the implementation of a nominated bodies scheme whereby 'nominated bodies' such as 'expert charities' will be able to highlight systemic issues with relevant online services

Regulation Bill Submission to the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht (March 2021).

[22] Houses of the Oireachtas, Joint Committee on Tourism, Culture, Arts, Sport and Media debate, General Scheme of the Online Safety and Media Regulation Bill: Discussion (Resumed) (14 July 2021) <https://www.oireachtas.ie/en/debates/debate/joint_committee_on_tourism_culture_arts_sport_and_media/2021-07-14/3/?highlight%5B0%5D=online&highlight%5B1%5D=safety&highlight%5B2%5D=media&highlight%5B3%5D=regulation&highlight%5B4%5D=bill > accessed 22 February 2022.

[23] Irish Council of Civil Liberties, ICCL submission on the Online Safety and Media Regulation Bill To: Oireachtas Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht Date (8 March 2021).

[24] Ombudsman for Children, General Scheme of the Online Safety and Media Regulation Bill 2020, Submission by the Ombudsman for Children's Office to the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht (4 March 2021).

[25] ibid.

[26] Department of Communications, Climate Action & Environment, *Thematic Analysis - Public Consultation on the Regulation of Harmful Online Content and the Transposition of the Audiovisual.*

and designated online services to the Media Commission/OSC. However, the systemic approach and lack of an individual complaints mechanism may create a barrier for victims of IBSA and result in the under reporting of issues in cases where individuals are unhappy with the results obtained from a provider's reporting process.[27]

Head 50B to Head 56 of the General Scheme of the Bill provided for the Media Commission to regulate harmful online content, however, there was no role for the Media Commission/OSC in regard to individual complaints and crucially in relation to the takedown of IBSA or harmful content following an individual complaint. Supporting material to the General Scheme stated that the 'proposed regulatory framework for online safety is systemic in nature and, as such, it does not contain a mechanism solely designed for an individual person to report individual pieces of potentially harmful online content to the OSC for assessment and potential action.'[28] While the Media Commission/OSC was designed to have the power to conduct investigations and inquiries into designated online services' compliance with safety codes, the General Scheme of the OSMRB failed to provide a mechanism for individuals to appeal to the Commission when a social media site failed to comply with the safety codes or to report harmful content such as intimate images. The Department did not consider it feasible to introduce a mechanism for individual complaints for a number of reasons as outlined in the Policy Paper 5[29] and Dáil Debates[30] including 'poor scalability and effectiveness'.[31] In particular, the Minister for Tourism, Culture, Arts, Gaeltacht, Sport and Media, Catherine Martin provided the following points as justification for a lack of an individual reporting mechanism in the Bill as follows:

- requirements for fair procedures would not facilitate a swift resolution of individual issues, as it would be necessary to engage with the uploader of content as well as the complainant;
- the volume of online content, particularly as Ireland will be regulating Video Sharing Platform Services for the whole of the EU population of 450 million

[27] The Institute for Future Media, Democracy and Society (FuJo) and the National Anti-Bullying Research, The General Scheme of the Online Safety and Media Regulation Bill Submission to the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht (March 2021).

[28] Government of Ireland, Online Safety and Media Regulation Bill, Summary of the virtual workshop on the regulatory framework for online safety (18 June 2020) 19.

[29] Government of Ireland, Regulatory Impact Assessment, Online Safety and Media Regulation Bill (November 2020) Policy Paper 5, 26.

[30] Dáil Éireann Debate 'Online Safety' (15 June 2021) < https://www.oireachtas.ie/en/debates/question/2021-06-15/540/?highlight%5B0%5D=media&highlight%5B1%5D=online&highlight%5B2%5D=safety&highlight%5B3%5D=media&highlight%5B4%5D=regulation&highlight%5B5%5D=bill&highlight%5B6%5D=online&highlight%5B7%5D=online#pq-answers-540_541 > accessed 22 February 2022.

[31] Government of Ireland, Regulatory Impact Assessment, Online Safety and Media Regulation Bill (November 2020) Policy Paper 5, 26.

people, would overwhelm even the best resourced regulator and divert resources away from regulatory oversight;
- referring complaints relating to individual items of content that are potentially criminal in nature to a civil regulator instead of An Garda Síochána would not be appropriate; and
- it would incentivise regulated online services to refer matters to the regulator rather than to take responsibility for resolving the matter themselves.[32]

Technology Ireland supported this view of the Government stating that an individual complaints system would be 'ineffective and administratively unworkable' stating:

> It [individual complaints system] would not deliver better outcomes for citizens and users of online services, as the number of complaints the Commission could expect to pursue would necessarily be limited, and time and resources would be diverted from pursuing systemic improvements in online safety for all.[33]

While the Government provided some explanation for its reasoning at the time, their arguments were strongly disputed. Key stakeholders such as Children's Rights Alliance, the Law Society of Ireland, the Institute for Future Media, Women's Aid, the Ombudsman for Children, and the Dublin Rape Crisis Centre all expressed concern and advocated for the necessity of some form of individual complaints mechanisms to assist with removal or to act as an appeal body for non-compliance of social media platforms.[34]

As outlined in Chapter 4 section 4.2.2.2, the LRC recommended establishing a statutory DSC, modelled on the Australian OESC.[35] The LRC also envisioned that this office would

---

[32] Dáil Éireann Debate 'Online Safety' (15 June 2021) < https://www.oireachtas.ie/en/debates/question/2021-06-15/540/?highlight%5B0%5D=media&highlight%5B1%5D=online&highlight%5B2%5D=safety&highlight%5B3%5D=media&highlight%5B4%5D=regulation&highlight%5B5%5D=bill&highlight%5B6%5D=online&highlight%5B7%5D=online#pq-answers-540_541 > accessed 22 February 2022.

[33] Technology Ireland, submission on the General Scheme of the Online Safety and Media Regulation Bill (8 March 2021).

[34] Children's Rights Alliance, Submission to the Joint Oireachtas Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht on the General Scheme of the Online Safety and Media Regulation Bill (8 March 2021); Law Society of Ireland, Submission on the General Scheme of the Online Safety and Media Regulation Bill, Oireachtas Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht (18 March 2021); Women's Aid, Submission to the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht on the General Scheme of the Online Safety and Media Regulation Bill (March 2021); The Institute for Future Media, Democracy and Society (FuJo) and the National Anti-Bullying Research, The General Scheme of the Online Safety and Media Regulation Bill Submission to the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht (March 2021); Dáil Éireann Debate, Joint Committee on Tourism, Culture, Arts, Sport and Media debate, General Scheme of the Online Safety and Media Regulation Bill: Discussion (Resumed) (14 July 2021) < https://www.oireachtas.ie/en/debates/debate/joint_committee_on_tourism_culture_arts_sport_and_media/2021-07-14/3/?highlight%5B0%5D=online&highlight%5B1%5D=safety&highlight%5B2%5D=media&highlight%5B3%5D=regulation&highlight%5B4%5D=bill> accessed 22 February 2022.

[35] Law Reform Commission, *Harmful Communications and Digital Safety (LRC 116 — 2016)*144.

have responsibility for publishing a Code of Practice on Digital Safety which would include an efficient take-down procedure.[36] Under the LRC proposals, if a social media site did not comply with the standards in the Code of Practice, an individual could then appeal to the DSC, who could direct a social media site to comply with the standards in the Code.[37] The LRC further recommended that if a social media site did not comply with the DSC direction, the Commissioner could apply to the Circuit Court for a court order requiring compliance.[38]

Under the General Scheme of the Online Safety and Media Regulation Bill, there was no direct avenue for redress for an individual who is the subject of harmful online content abuse such as IBSA. In the LRC Report on Harmful Communications and Digital Safety, the importance of an accessible and effective takedown mechanism to remedy victims of online abuse such as IBSA was highlighted:

> The Report acknowledges that available processes and remedies may not be effective, and that the potential cost, complexity and length of civil proceedings may prevent victims of harmful digital communications from obtaining redress in court. A victim of harmful communications should be able to have a readily accessible and effective takedown procedure available to him or her.[39]

As explained in Chapter 4 section 4.2.2.2, the LRC recommended that:

> The Office of the Digital Safety Commissioner of Ireland should be established to promote digital and online safety as well as overseeing and regulating an efficient and effective procedure for takedown of harmful digital communications.[40]

It is evident from the General Scheme that this specific recommendation had been eschewed.[41] As a result, the Law Society of Ireland recommended that the General Scheme of the Bill should include the LRC recommendation that there be a body 'overseeing and regulating an efficient and effective procedure for takedown of harmful digital communications' so that individuals have an immediate remedy in the event of a failure of an online service to provide a system of complaint that adheres to the standards of the online safety codes.[42]

---

[36] ibid.
[37] ibid.
[38] ibid.
[39] ibid 10.
[40] Ibid 141, 142.
[41] Law Society of Ireland, Submission on the General Scheme of the Online Safety and Media Regulation Bill, Oireachtas Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht (18 March 2021).
[42] ibid.

Although IBSA had been criminalised under the Harassment, Harmful Communications and Related Offences Act 2020, criminal prosecutions may take time and, for a variety of reasons, do not always proceed.[43] Furthermore, the priority for victims of IBSA victims is to first regain control of their image and limit its distribution. The prosecution of perpetrators is often seen as a secondary goal.[44] As a result a 'fast, free and effective way'[45] to compel the removal of harmful content (including IBSA) where service providers' mechanisms have failed is necessary.

While the Law Society of Ireland supported the LRC model of a Digital Safety Commissioner, Women's Aid promoted the Australians' eSafety Commissioner's approach as a faster more efficient mechanism for speedy removal. As explained in Chapter 2 and 3, the Australian OESC has a number of roles, including education and guidance, research, coordination, responding to complaints of cyber-bullying against children, responding to complaints about illegal and harmful content, and responding to complaints about IBSA.[46] This includes providing users with the option of making a report online to the IBA portal which facilitates rapid removal of the images. Unlike the LRC proposed DSC approach whereby a victim must first request removal of the intimate image through the social media platform, in Australia the victim only has to make a report to the OESC and does not have to deal with the online services where the harmful content is posted which can be very 'distressing'.[47] Women's Aid argued that the OSC in Ireland should have an active role in having IBSA and other harmful content removed, or at least have an appeal role as envisaged in the LRC Report.[48] Furthermore, the Institute for Future Media expressed concern that the lack of provision for an individual complaints mechanism may lead to an 'underreporting of issues' in cases where individuals are

[43] Women's Aid, Submission to the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht on the General Scheme of the Online Safety and Media Regulation Bill (March 2021).
[44] Nicola Henry, Asher Flynn & Anastasia Powell, 'Policing image-based sexual abuse: stakeholder perspectives' (2018) 19(6) Police Practice and Research 565
[45] Women's Aid, Submission to the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht on the General Scheme of the Online Safety and Media Regulation Bill (March 2021).
[46] eSafety Commissioner, 'What We Do' < https://www.esafety.gov.au/about-us/what-we-do > accessed 22 February 2022.
[47] Women's Aid, Submission to the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht on the General Scheme of the Online Safety and Media Regulation Bill (March 2021).
[48] Women's Aid, Submission to the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht on the General Scheme of the Online Safety and Media Regulation Bill (March 2021). See 'Recommendation 4: That the role of the Online Safety Commissioner is expanded to include responding to individual complaints of image-based abuse and other harmful content and facilitating their removal. Failing that, that the Online Safety Commissioner would at least have an appeal role in relation to takedown requests, as in the Law Reform Commission report'.

unhappy with the results obtained from a provider's reporting process, therefore leaving victims powerless.[49]

5.2.4 Specific issues with the nominated bodies complaints scheme

While the General Scheme granted the Commission authority to create a nominated body complaints system, it provided very limited information on how this system would operate in practice. It failed to specifically outline which specific bodies would be considered 'nominated bodies', what types of expertise such bodies would need to have, and how these bodies would determine which complaints or issues should be notified to the Media Commission. As stated by Technology Ireland there was 'no guidance' in the General Scheme of the Bill as to the 'circumstance in which a nominated body may submit a complaint.'[50] The Ombudsman for Children described this absence of 'clarity' as 'problematic' as it made it a challenge to assess whether or not the complaints system was appropriate and likely to be effective.[51] Head 53 explained that where the Commission issued a compliance notice following an investigation into a complaint made via the nominated bodies complaints scheme, the issuing of that compliance notice would have to follow certain steps. Firstly, the compliance notice would have to outline the Media Commission's views and how it formed those views. It would outline the steps the Media Commission/OSC deemed necessary for the designated online service to take to bring itself into compliance which may include changing a system or policy, or the removal or restoration of content, and the timescale in which those steps must be taken.[52] If the steps to be specified in a compliance notice are related to the removal or restoration of material the Media Commission would be entitled to invite submissions from the uploader and complainant before it issues the notice.[53] While these steps addressed the need for due process, by ensuring necessary checks before content is removed so to avoid the removal of legitimate content and also provide an opportunity for the uploader to defend his/her post, the process as designed would be time consuming and could cause

[49] The Institute for Future Media, Democracy and Society (FuJo) and the National Anti-Bullying Research, The General Scheme of the Online Safety and Media Regulation Bill Submission to the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht (March 2021).
[50] Technology Ireland, submission on the General Scheme of the Online Safety and Media Regulation Bill (8 March 2021).
[51] Ombudsman for Children, General Scheme of the Online Safety and Media Regulation Bill 2020, Submission by the Ombudsman for Children's Office to the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht (4 March 2021).
[52] General Scheme of the Online Safety and Media Regulation Bill, Head 53 (2) (3).
[53] ibid.

harmful material such as intimate images to spread online and leave a victim of IBSA with no control over their image and make the task of regaining control of their image impossible.

An alternative solution would be to require the OSC to first order the removal or temporary restriction of the potential intimate image/harmful content and then after invite submissions and make a determination which would be subject to an appeal to the court. If the content was deemed harmful then it would already have been removed before further harm was caused. If the content was deemed legitimate, the content could be reposted so to uphold the uploaders right to freedom of expression. In order to ensure that such a system does not result in disproportionate restrictions, the system and its safeguards would have to be carefully designed. In situations where IBSA material is being hosted, there is a particularly strong argument for immediate removal pending appeal as there is little identifiable public interest associated with such material and the nature of the material makes the speedy removal of the content particularly important if the harm is to be adequately mitigated. Regardless of improvements that could be made to the nominated bodies systemic complaints system, the fact that the system establishes nominated bodies as gatekeepers – creating a barrier between individuals and the OSC – is problematic in the absence of an individual mechanism. A clear path for victims or an individual on behalf of a victim to report to the OSC would be empowering and would also have a clear symbolic effect.

5.2.5 Issues with the obligation to consider mediation

Head 52C provided for an obligation to consider mediation in case of a dispute between a user and an online service provider. This section lacked clarity as it was unclear what type of cases might require mediation. Furthermore, in the absence of an individual complaints mechanism, end-users dissatisfied with a platform provider's response may be 'deterred' from pursuing this further if the option provided to them is a 'complicated' and a potentially 'costly' mediation process with no clarity as to how a decision is made as to who covers the costs/percentage of costs.[54] Women's Aid expressed concern for this mediation obligation in relation to cases of IBSA as the obligation to engage in mediation may prolong proceedings further while the intimate image remains available online and

[54] The Institute for Future Media, Democracy and Society (FuJo) and the National Anti-Bullying Research, The General Scheme of the Online Safety and Media Regulation Bill Submission to the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht (March 2021).

can be accessed, shared and downloaded.[55] Overall, such a process offers little benefit to victims of IBSA.

5.2.6 The merits of an intermediate goal

Under the framework, the Media Commission/OSC would have to follow a lengthy process before seeking an order to ensure the removal of a piece of content. The Media Commission/OSC would have to investigate, issue a warning notice, issue a compliance notice and then finally seek a court order to impose a sanction. The legislation also did not set out any time frames upon which any of these processes would have to be completed within. An intimate image could be distributed widely as these processes were worked through. As a result, there is a need for an intermediate action. For example, Women's Aid suggested that reported intimate images should be taken down within a fixed time period during any dispute proceedings until the dispute is resolved as a precaution against further sharing of the content.[56] Officials from the Department for Communications, Climate Action and Environment[57] were asked during the virtual workshops whether material flagged as harmful online content should be required to be removed as a default prior to any assessment of whether or not it falls within the categories of harmful online content.[58] The 'Department's response' acknowledged that this may be possible in relation to content that is a criminal offence to disseminate such as intimate images however may not be possible for material which is harmful yet not a criminal offence to disseminate.[59] The Department for Communications, Climate Action and Environment justified their response by explaining that the balancing of rights in the latter circumstance may pose legal challenges.[60] As a result, the 'Department's response' stated that a measure to allow default removal orders by the Media Commission/OSC would be 'unlikely'.[61] Such a measure would be extremely helpful in cases of IBSA considering how much value victims typically place on regaining control of their image

[55] Women's Aid, Submission to the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht on the General Scheme of the Online Safety and Media Regulation Bill (March 2021).
[56] Women's Aid, Submission to the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht on the General Scheme of the Online Safety and Media Regulation Bill (March 2021).
[57] The report does not specify which officials, only that the then Minister for Communications, Climate Action and Environment Richard Bruton was in attendance.
[58] Government of Ireland, Online Safety and Media Regulation Bill, Summary of the virtual workshop on the regulatory framework for online safety (18 June 2020) 22.
[59] ibid.
[60] ibid.
[61] ibid.

and also considering the potential challenges with securing a criminal prosecution under the new targeted legislation as highlighted in Chapter 4 section 4.3.3.

5.2.7 Transparency for reporting mechanisms

As evidenced in Chapter 4 section 4.2, the self-regulation of intermediaries within Ireland has been unsuccessful in the context of IBSA. An important element of successful self-regulatory approaches is robust reporting mechanisms and speedy removal of harmful content.[62] However issues arise when companies do not remove the harmful material rapidly enough or in some cases at all.[63] As a result the imposition of Online Safety Codes to ensure platforms have robust reporting mechanisms for harmful content such as IBSA and that the OSC would have the ability to audit and investigate the effectiveness of platform reporting mechanisms would be positive developments. Any system of this nature must be implemented in a rights compliant manner.[64] Crucially, transparency as to how the effectiveness of a platform's reporting mechanism is assessed and whether or not it is satisfying the Online Safety Codes will be essential.

5.2.8 The importance of sanctions but the need for safeguards

Head 54A set out that the Media Commission would apply a range of sanctions to a designated service provider for non-compliance with a warning notice. Head 54A(5) stated:

> The Commission may seek to apply any of the following sanctions:
> (a) an administrative financial sanction in accordance with the procedure set out in Head 16.
> (b) to seek leave of the High Court to compel a designated online service subject to a warning notice under this section to take such steps that the Commission deems warranted to bring said service into a state of compliance, or,
> (c) to seek leave of the High Court to compel internet service providers to block access to a designated online service in the State.[65]

[62] Tarleton Gillespie and others, 'Expanding the Debate About Content Moderation: Scholarly Research Agendas for the Coming Policy Debates' (2020) 9(4) Internet Policy Review; Robert Gorwa, Reuben Binns, & Christian Katzenbach, 'Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance' (2020) 7(1) Big Data & Society.
[63] Tijana Milosevic & Marko Vladisavljevic, 'Norwegian Children's Perceptions of Effectiveness of Social Media Companies' Cyberbullying Policies: An Exploratory Study' (2020) 14(1) Journal of Children and Media 74.
[64] The Institute for Future Media, Democracy and Society (FuJo) and the National Anti-Bullying Research, The General Scheme of the Online Safety and Media Regulation Bill Submission to the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht (March 2021).
[65] General Scheme of the Online Safety and Media Regulation Bill, Head 54A.

The explanatory note to this section stated that 'the application of each of these sanctions requires court approval whereupon the designated online service in question will have the opportunity to dispute its application'.[66]

The LRC described the power to impose administrative financial sanctions as 'one of the most effective in the regulatory toolkit' and that the power to impose administrative financial sanctions is both 'valuable and necessary' in ensuring that financial and economic regulators have the requisite powers to achieve their regulatory objectives.[67] Under the General Scheme of the Bill, the Media Commission would be granted the ability to impose administrative financial sanctions and seek the removal of content. Once the Media Commission decided that a contravention had occurred, whereby a service provider has failed to comply with a compliance or warning notice issued by the Media Commission, the Media Commission would first notify the service provider in writing of the decision to impose an administrative financial sanction or other sanction such as a notice for removal and the reasons for the decision. The provider could either accept the decision or appeal the decision. In the context of administrative financial sanctions, the provider could appeal to the Circuit Court if the amount did not exceed €75,000 or the High Court if the amount was over €75,000 for review. If the service provider accepted the decision and did not appeal, the Media Commission would make an application in a summary manner to the Circuit Court for confirmation of the decision. Any decision, including the amount of the sanction in the context of administrative financial sanctions or whether a sanction applies, would be subject to court review.[68] Traditionally, regulatory bodies were not allowed to avail of such powers due to the rights balancing issues such as the provision of due process however following the decision in *Purcell v. Central Bank*[69] such sanctions are permissible where they do not constitute the administration of justice by a non-court entity. The General Scheme of the Bill ensures this safeguard by ensuring any sanction permitted under the Bill can be subject to an appeal.

A regulatory body without the ability to impose such sanctions would be ill-equipped to enforce any safety codes or execute its mission, purpose or functions. However, the process of seeking a court order to issue a compliance notice or to compel internet service

[66] ibid Head 54A explanatory note.
[67] The Law Reform Commission, *Report on Regulatory Powers and Corporate Offences* (LRC 119-2018).
[68] Government of Ireland, General Scheme of the Online Safety and Media Regulation Bill Q&A 13.
[69] *Purcell v. Central Bank* [2016] IEHC 514.

providers to block access to a designated online service in the State could result in delays that could result in additional harm. As a result, consideration must be given to a more empowered Media Commission with the ability to make a determination and impose a sanction in these contexts without the need for a court order but which can later be appealed to a court. Such an option would likely not be appropriate in all circumstances; but in the context of IBSA, it is contended that the irreversible nature of the harm caused by delayed processes combined with the strong factual evidence that the subject of an intimate image does not wish for it to be shared could justify a more proactive approach to content removal once sufficient safeguards are provided for.

5.2.9 Collaboration

During the virtual workshop held on the 18th of June 2020, issues were raised around how the Media Commission/OSC would interact with other already established bodies/organisations who deal with similar matters outlined under the General Scheme of the Bill. In response to this issue, the Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media published in a questions and answers document that it was intended that there would be a 'memoranda of understanding' between the Media Commission and other relevant bodies, such as An Garda Síochána and the Data Protection Commission, to allow these organisations to set out appropriate boundaries in their activities and to ensure an appropriate amount of cooperation in instances where their activities may overlap.[70] Furthermore the Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media in the questions and answers document further highlighted that the role of the OSC would be to 'regulate online services and not the activities of users' therefore it would not replace but complement the roles of existing regulators.[71] This approach and level of collaboration would require clear organisation and communication between all bodies to ensure victims do not get confused about which organisation they should be dealing with and at what point and to ensure each body is fully aware of the other bodies' functions and powers so that they can direct victims to the appropriate body. There is a risk that there may be too many entities involved for victims and that a 'one stop shop' for victims may be more appropriate.

5.2.10 The need for greater educational and awareness raising functions

[70] Government of Ireland, General Scheme of the Online Safety and Media Regulation Bill Q&A 7.
[71] ibid.

As stated by Assistant Garda Commissioner John O'Driscoll, online crime is progressing at 'an incredibly fast pace', with new trends constantly emerging.[72] Online criminals are becoming more 'agile, exploiting new technologies with lightning speed, tailoring their attacks using new methods, and co-operating with each other in ways we have not seen before'.[73] These crimes know no borders, cause serious harm and pose very real threats to victims worldwide. As a result, there is a great need to educate people and raise awareness around online crimes such as IBSA so to reduce perpetration levels and inform victims of supports and avenues of complaint available to them. Children's Rights Alliance, the Ombudsman for Children, and Women's Aid highlighted that the General Scheme of the Bill 'appears to be otherwise silent' on the awareness raising and education functions of the Commission, including with regard to online safety.[74] They expressed concern that the General Scheme did not provide for the Commission to evaluate or regulate educational and community awareness programmes about online safety.[75]

5.3 Application of lessons learned from Australia

While the above assessment of the OSC provides some insight into the potential merits and limitations of the Irish regulatory response as was proposed at that time under the General Scheme of the OSMRB, there is an opportunity to learn from the Australian OESC and apply the lessons learned from this established approach so to improve the Irish response to IBSA. A key aim of Chapters 2 and 3 was to identify lessons from the desk-based assessment and interviews conducted on the functioning of the OESC in order to later analyse these lessons in the Irish context and inform the Irish response to IBSA. As a result, the purpose of this section is to analyse the current Irish situation in the context of IBSA while using the lessons learned from Australia in order to identity the merits and

[72] Dáil Éireann Debate, Joint Committee on Tourism, Culture, Arts, Sport and Media debate, General Scheme of the Online Safety and Media Regulation Bill: Discussion (Resumed) (14 July 2021) < https://www.oireachtas.ie/en/debates/debate/joint_committee_on_tourism_culture_arts_sport_and_media/2021-07-14/3/?highlight%5B0%5D=online&highlight%5B1%5D=safety&highlight%5B2%5D=media&highlight%5B3%5D=regulation&highlight%5B4%5D=bill> accessed 22 February 2022.

[73] ibid.

[74] Children's Rights Alliance, Submission to the Joint Oireachtas Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht on the General Scheme of the Online Safety and Media Regulation Bill (8 March 2021); Ombudsman for Children, General Scheme of the Online Safety and Media Regulation Bill 2020, Submission by the Ombudsman for Children's Office to the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht (4 March 2021); Women's Aid, Submission to the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht on the General Scheme of the Online Safety and Media Regulation Bill (March 2021).

[75] Children's Rights Alliance, *Report Card 2021* (2021) 213.

demerits of the Irish approach while also highlighting recommendations for reform. This section aims to provide clear recommendations on how best to tackle IBSA and how best to establish an avenue of redress for IBSA victims (informed by the extensive study of the Australian approach) in the hope that these recommendations may influence policy decisions and future legislation, including the OSMRA. Some of the lessons learned from the Australian experience provide clear guidance on best practice while others flag areas of concern. However, both provide Ireland with an opportunity to learn from the successes while avoiding the weaknesses, as discussed below. This discussion is broken down into eight key headings as follows:

1. An empowered regulator
2. A victim-centred approach – the need for an individual complaints system
3. Preventive versus solely responsive – the need for educative and awareness raising functions
4. Collaboration and overlapping processes
5. International collaboration
6. The importance of transparency
7. Visibility
8. Independence

5.3.1 An empowered regulator

A core strength of the Australian OESC is the ability to impose removal notices and apply for court orders to impose fines and penalties. A key lesson learned from the Australian approach is that awareness campaigns and the mere ability to request the removal of harmful content without any power to enforce such requests are unsuccessful in achieving actual results and therefore the expanded powers of the OESC in 2018 to include a civil penalty regime to assist in the removal of IBSA through fines was imperative.[76] This statutory power allows the OESC to be viewed as an empowered enforcer. The mere ability to impose a sanction encourages individuals and intermediaries to remove intimate images upon request.[77] Without such a statutory power, the OESC may be accused of having no 'backbone'.[78] Furthermore, the success of the OESC statutory power is evident

[76] See Chapter 2 section 2.3.8.1 & section 2.4.1.
[77] Interview with 'OESC representative 1', Melbourne Central Tower, (Melbourne, 2019) See Chapter 3 section 3.6.2.3.
[78] Interview with Nicola Henry, Academic, RMIT, (Melbourne, 2019). See Chapter 3 section 3.6.2.3 'I think the Australian model is a good one because the statutory legislation behind it does give it weight and

through its increased removal rate following its the expansion of its powers. Following the implementation of the civil penalty regime, the removal rate of intimate images by the OESC increased from 80% to 90%.[79] While 80% could be considered an impressive removal rate based upon voluntary request, the ability to take enforcement action further improved the OESC success rate in assisting in the removal of intimate images. Moreover, the prospect of forthcoming expanded powers would likely be an incentive for service providers to engage in cooperation from the outset. As a result, a strong merit of the Australian system is the statutory power granted to the OESC. Fortunately, a version of this feature has been adopted in the Irish approach. While the OESC has not yet imposed penalties for non-compliance with its removal notices, the ability to act enhances voluntary compliance from intermediaries, social media services and end-users. Without such power there would be less compliance as seen prior to the OESC expanded power.

While it is clear that an internet regulator must be an empowered body, analysis of the Australian approach also uncovered some limitations around the implementation of such powers which must be considered in the Irish context. Firstly, while the ability to issue notices and sanctions leads to increased cooperation and more efficient self-regulatory policies, the Australian approach highlighted that a significant problem exists with 'outlier' services where the issues of identifiability and location arise unlike with the large and prominent internet companies. Due to this, some smaller platforms or websites are somewhat insulated from the powers of the OESC. A significant number of these 'outliers' are based in jurisdictions beyond the jurisdiction of the OESC. As a result, where statutory power is ineffective the OESC resorts to a useful mitigation measure which is to either request the content be de-indexed from a search engine or issue a link deletion notice to ensure the reduced visibility of the content.

> In the very unusual circumstance where we can't get content removed … our failsafe is always we can de-index from Google search results so that way even if we're unable to get the content removed, we know that we minimize the exposure. People can't search for it. ('OESC representative 1')

I fear that you know an agency that set up that doesn't have any weight that doesn't have any power, that's purely symbolic and kind of plays an indicative function would just lack a back bone'.

[79] Interview with 'OESC representative 1', Melbourne Central Tower, (Melbourne, 2019). See Chapter 3 section 3.6.2.3 'It might just be a question of correlation rather than causation but when we start in October 2017 prior to the civil scheme starting, our removal success rate was around 80 percent. And for the last financial year or since the scheme started, it is at 90 per cent now. So that could be for a range of factors, it could be growing awareness of us and our powers, it could be content providers being a little bit scared of them or it could just be that we're getting better at what we do, and that we're tenacious'.

The General Scheme of the Irish Bill lacked consideration for situations where statutory powers are ineffective. While the OESC at the time of the interviews discussed in Chapter 3 did not have this mitigation measure specifically provided for in the legislation, the OESC utilised voluntary requests. Since those interviews were conducted, the Online Safety Act has been passed and now formal provision has been made for link deletion notices. While the Irish approach allows the Media Commission/OSC to seek a court order to compel an internet service provider to block access to a designated online service in the State who fails to comply with a warning notice, this sanction may lead to the removal of legitimate content and would likely be used very sparingly as a result. Ireland should learn from Australia's actions and include a mitigation measure through the means of a link deletion notice which targets the harmful content specifically. Such a measure will protect against the restriction of legitimate content while ensuring that the visibility of harmful content such as intimate images is reduced therefore reducing the harm caused to victims in the absence of a possibility for complete removal.

Another limitation regarding the OESC statutory powers is that the process of applying for a court order to force compliance with a notice or for permission to impose a sanction is 'very slow' and may take weeks according to interview participant Peter Clarke.[80] Based on this experience, it is suggested that a form of injunctive relief is a more appropriate approach as the image can be removed immediately and then reposted if no harm is found.[81] This approach should be considered in the Irish context for content that is a criminal offence to disseminate. If the OSC has the power to immediately issue a removal notice and afterwards seek a court order, the intimate image can be quickly removed before it receives greater exposure. Retaining the obligation to seek a confirmative order – and allowing a right of appeal – should mitigate the risk of legitimate content being removed. Due to the potential risk to freedom of expression, it is essential that such a power be tightly constrained and that clear processes for determining whether content is prima facie illegal be established.

[80] Interview with Peter Clare, Legal Practitioner, (Melbourne, 2019). See Chapter 3 section 3.6.2.3.

[81] Interview with Peter Clarke, Legal Practitioner, (Melbourne, 2019) See Chapter 3 section 3.6.2.3 'The more important action that should be taken is some form of injunctive relief. And then you can bring a civil penalty proceeding because injunctive relief is basically saying remove it. Then we'll sort out the nature of the ill or whether it should be returned. Because ultimately the matter is about dealing with the problem immediately because it has an immediate impact on the victim'.

5.3.2 A victim-centred approach – the need for an individual complaints system

While Head 50B to Head 56 of the General Scheme of the Bill provided for the Media Commission to regulate harmful online content, the General Scheme of the Bill allowed no role for the OSC in regard to individual complaints and crucially in relation to the takedown of IBSA following an individual complaint. As a result, the regulatory framework for online safety was entirely 'systemic in nature' and, as such, did not contain a mechanism for an individual to complain to the Media Commission when a social media site failed to comply with the safety codes or to report harmful content such as intimate images.[82] While the systemic approach has its merits and should facilitate the high level assessment of systems and online environments and assist the regulator in identifying and addressing systemic issues, there is a need for an individual complaint mechanism so to ensure an additional targeted avenue of redress for victims of IBSA.

The systemic approach is in contrast to the regulatory framework in Australia whereby the OESC provides individual reporting mechanisms for IBSA, harmful online content, and cyberbullying material whereby individuals can seek direct help from the OESC to help remove harmful content or to report the failure of a platform in removing such content. Furthermore, it is in contrast to the LRC framework of providing a DSC which would act as an appeals body whereby an individual could seek help for the removal of content which had failed to be removed by a platform following a report.

The importance of this individual complaints aspect for IBSA victims through the OESC IBA portal was greatly highlighted during the analysis conducted in Chapters 2 and 3. In particular, the availability of an individual complaints mechanisms was regarded as necessary as it acts as a supplementary avenue of redress for the removal of harmful content as opposed to a criminal approach or a traditional civil approach which can be slow, expensive and re-traumatising for victims.[83] The Australian OESC removal processes adopts a victim-centred approach as these processes are not primarily aimed at punishing a perpetrator but rather about the removal of harmful content.[84]

Based on the analysis conducted in Chapter 2 and 3, the majority of stakeholders within Australia (including stakeholders from the desk-based assessment and interviews) are

[82] Government of Ireland, Online Safety and Media Regulation Bill, Summary of the virtual workshop on the regulatory framework for online safety (18 June 2020) 19.
[83] Interview with Nicola Henry, Academic, RMIT, (Melbourne, 2019); Interview with Helen Campbell, Executive Officer Women's Legal Service NSW, Melbourne City University (Melbourne, 2019); Interview with Nicolas Suzor, Academic, Online, (Melbourne, 2019).
[84] Interview with Bianca Fileborn, Academic, (Melbourne, 2019).

supportive of the IBA reporting mechanism as it provides victims with a timely, accessible, and effective means of redress not available to them through the criminal justice system. Feedback from police submissions within Australia prior to the establishment of the IBA reporting mechanism indicated that victims were often reluctant to pursue criminal charges against perpetrators, as it could result in lengthy and onerous court processes, which resulted in amplifying the harm inflicted on the victim. Therefore, the IBA reporting mechanism administered by the OESC was seen as a welcome avenue of redress. Furthermore, the Australian experience highlights how victims struggle to articulate their concerns to platforms and therefore the OESC has greater impact than an individual when approaching a platform with a removal request.[85]

Chapter 4 section 4.2 demonstrates how victims of IBSA in the past were let down by An Garda Síochána in Ireland when seeking to regain control of their intimate image and the targeted legislation criminalising IBSA may pose evidential challenges for An Garda Síochána when trying to bring a case. As a result, there is a need for a more victim-centred approach with a focus on the speedy removal of intimate images. This task would be more appropriately carried out by an alternative body such as the OSC rather than An Garda Síochána or a lengthy court process. Providing a service that is free and accessible is regarded as highly beneficial for victims as it provides a safe avenue to report cases and reduces trauma. Furthermore, research commissioned by the eSafety Commissioner explains that 72% of women believe it is 'futile' to make a report to a social media platform as they believe nothing will be done.[86] As a result, an alternative route to the traditional police or court process or social media complaints handling systems is beneficial considering that some victims are reluctant to report to the traditional channels.

Ireland's system needs to include the ability for the OSC to accept and respond to individual complaints or to expand the role of the systemic complaints system to allow for individual complaints. While a victim of IBSA may want to report a case of IBSA so to ensure the removal of the image by the end user or prevention of the posting of the image by the end user in the first place, a victim may also want to ensure their image is not being hosted on a platform. Furthermore, a person may at one stage have consented to the posting of an intimate image of them but later would like to retract that consent. As

[85] Interview with Nicolas Suzor, Academic, Online, (Melbourne, 2019).

[86] Based on a mixed method study and survey of women who were working or have worked in the past three years, and who were online or in the media for work purposes. 1491 women were surveyed and 20 individual interviews were conducted from May to July 2021. eSafety Commissioner, ' Women In The Spotlight: How online abuse impacts women in their working lives' <https://www.esafety.gov.au/about-us/research/how-online-abuse-impacts-women-working-lives# > accessed 22 February 2022.

a result, the OSC requires an individual complaints mechanism which would allow for the reporting of an intimate image without consent but also the ability to object to the hosting of an image which was once consensual but later the consent retracted. Australia accounts for this distinction by allowing individuals to issue an objection notice or a complaint. There is a necessity for the OSC to have some form of individual complaints mechanism to allow for the reporting of IBSA material and to assist with removal of such content or to at least act as an appeals body for non-compliance of social media platforms whereby victims can report to the OSC where they have been unsuccessful in having their intimate image removed by a host platform.[87]

5.3.3 Preventative versus solely responsive – the need for a balance between educative and awareness raising functions

The Australian OESC balances practicing a role of education and awareness raising alongside a role of enforcement when combating online regulation in the context of IBSA. In particular the OESC provides an array of educational tools and resources to a wide-ranging audience across Australia. These resources aim to educate perpetrators, victims, students, family, friends, frontline workers, and bystanders. Chapter 2 and Chapter 3 demonstrate how the educative functions of the OESC hosted through its website including the IBA portal and the virtual classrooms and workshops raise awareness and understanding of the harms of online crimes such as IBSA while also assisting victims in identifying clear avenues for redress. According to Third, the eSafety Commissioner's website is a 'focal point for online safety issues'[88] and is a 'trusted portal' for access to 'high quality' online safety resources.[89] While Head 10 of the General Scheme stated that the Media Commission would have a function to provide education around online safety,

[87] Children's Rights Alliance, the Law Society of Ireland, the Institute for Future Media, Women's Aid, and the Ombudsman for Children. Children's Rights Alliance, Submission to the Joint Oireachtas Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht on the General Scheme of the Online Safety and Media Regulation Bill (8 March 2021); Law Society of Ireland, Submission on the General Scheme of the Online Safety and Media Regulation Bill, Oireachtas Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht (18 March 2021); Women's Aid, Submission to the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht on the General Scheme of the Online Safety and Media Regulation Bill (March 2021); The Institute for Future Media, Democracy and Society (FuJo) and the National Anti-Bullying Research, The General Scheme of the Online Safety and Media Regulation Bill Submission to the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht (March 2021); Ombudsman for Children, General Scheme of the Online Safety and Media Regulation Bill 2020, Submission by the Ombudsman for Children's Office to the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht (4 March 2021).

[88] Amanda Third, 'Submission to the Review of the Enhancing Online Safety Act 2015 and the Online Content Scheme' (2018) 2.

[89] ibid.

there was a lack of guidance provided on how this would be conducted. Dáil debates, discussions and the virtual workshops fail to identify how the OSC's educative functions would be administered. There is a great need for an advanced interactive website which can serve various functions such as explaining in plain language the criminal law concerning IBSA and to educate the public on the extent of the issue and the harms caused as a result.

The General Scheme of the Bill provided no insight on the awareness raising and education functions of the Commission, including with regard to online safety.[90] There was no obligation within the General Scheme for the Commission to evaluate or regulate educational and community awareness programmes about online safety or to engage, promote or collaborate with such functions and campaigns already provided by key stakeholders of online safety regulation.

5.3.4 Collaboration and overlapping processes

The Australian experience has confirmed that while self-regulation alone is insufficient there is still a place for self-regulation alongside a body providing oversight. Collaboration is an essential practice of the OESC. Views expressed by five interview participants[91] in Chapter 3 suggested that the fostering of good relationships between the eSafety Commissioner and industry is useful when developing a collaborative approach to the regulation of the internet. According to 'OESC representative 1' as a result of the OESC developing good relationships with platforms and intermediaries, they have received high levels of compliance with their requests for content removal. As outlined in Chapter 2,[92] the Online Safety Act has provided for service provider notifications as a 'less formal approach' compared to a removal notice which are envisaged to result in faster content removal due to pre-established good relationships.[93] Furthermore, the major

[90] Children's Rights Alliance, Submission to the Joint Oireachtas Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht on the General Scheme of the Online Safety and Media Regulation Bill (8 March 2021); Ombudsman for Children, General Scheme of the Online Safety and Media Regulation Bill 2020, Submission by the Ombudsman for Children's Office to the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht (4 March 2021); Women's Aid, Submission to the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht on the General Scheme of the Online Safety and Media Regulation Bill (March 2021).

[91] Interview with 'OESC representative 1', 'OESC representative 2', & 'OESC representative 3', Melbourne Central Tower, (Melbourne, 2019); Interview with Christiane Gillespie-Jones, Communications Alliance, Online, (Melbourne, 2019); Interview with 'Alannah & Madeline Foundation representative 1', Clarendon Street South Melbourne, (Melbourne, 2019).

[92] See Chapter 2 section 2.5.3.6.1.

[93] Office of the eSafety Commissioner, *eSafety Regulatory Posture and Regulatory Priorities 2021-22* (November 2021).

platforms have ensured their self-regulatory policies are in line with the eSafety Commissioner's regulatory standards. As a result of the good rapport that the OESC have built with industry, which has led to stronger self-regulatory policies, this has reduced the need of the OESC to use the formal statutory powers which may result in speedier results and a more proactive approach by services.

While Chapter 3 demonstrated that all interviewees agreed that the eSafety Commissioner has fostered good relationships and collaboration with intermediaries and industry. Representatives from the Alannah and Madeline Foundation suggested that the OESC could engage in greater collaboration with NGOs. Representatives from the Alannah & Madeline Foundation believed the eSafety Commissioner could link more with NGOs as initiatives, policies, activities, programs, information, and education are too disjointed resulting in a lack of 'common understanding'.

The building of good relationships and the engagement in collaborative activities within Ireland will be essential in providing strong policies and compliance. Ireland's General Scheme of the Bill seems to have considered the importance of collaboration, with the legislation granting the OSC the ability to consult with key stakeholders in the administering of many of its functions. In particular, the creation of Online Safety Codes, guidance materials, and advisory notices, all allowed for the OSC to 'consult with any persons or bodies it sees fit'.[94] Furthermore, the systemic complaints system established under Head 52(B) allowed for 'nominated bodies' to bring forward complaints about systemic issues with relevant and designated online services. Consequently, it appears the system as initially set out in the General Scheme established avenues for collaboration with key stakeholders who could contribute to the provision of a safer online environment. However, while there are established avenues to engage in collaboration, there was no obligation on the OSC to carry out such activities and as a result it would be more beneficial to require the OSC to engage in collaboration so to ensure the development of positive relationships with the OSC and stakeholders within Ireland. Additional detail on the form such collaboration should take and how stakeholders will be identified should be provided for by law. Furthermore, the OSC must ensure that the reference to 'people', 'bodies' and 'nominated bodies' with whom they will collaborate with, allow for a wide array of stakeholders including platforms, intermediaries and

[94] General Scheme of the Online Safety and Media Regulation Bill, Head 50(A)(4), Head 51(A)(4), Head 51(B)(4).

NGOs so to avoid the exclusion of particular stakeholder groups as pointed out in the Australian context.

While collaboration is important within the Australian approach, the OESC is regarded as a 'one stop shop' for online safety support, guidance, and redress. This is in contrast to the approach in Ireland where the Government explained that it intended that there will be a 'memoranda of understanding'[95] between the Media Commission and other relevant bodies, such as An Garda Síochána and the Data Protection Commission, to ensure an appropriate amount of cooperation in instances where their activities may overlap.[96] This collaboration is particularly relevant in the Irish context as the role of the OSC will be to 'regulate online services and not the activities of users'[97] therefore it will not replace but complement the roles of existing regulators. The Irish approach was not set out in the General Scheme but was detailed in supporting documents and as a result there was a lack of clarity regarding how this level of collaboration would work in practice.

5.3.5 International collaboration

International collaboration is another key factor to consider when regulating IBSA. A key identified problem for the Australian OESC is the removal of content hosted overseas. Within the context of child sexual abuse material, established channels for international collaboration such as with INHOPE are essential for overcoming this issue. However, there is a lack of international collaboration for the removal of other content such as IBSA when hosted overseas. This is particularly an issue for content hosted on pornography sites hosted overseas. While this is a complex issue to solve, Ireland has made an attempt to reduce this issue by granting the OSC the ability to engage in voluntary arrangements with any relevant online service. This would mean that Ireland may approach an international platform and engage in discussions with that platform relating to compliance with Ireland's safety codes.[98] These arrangements would be made public. Following an arrangement, the OSC would be able to request information and determine reporting schedules for the platform.[99] The OSC could also make findings of non-compliance and publish the fact of these findings and to revoke arrangements if deemed necessary.[100] The

[95] Government of Ireland, Online Safety and Media Regulation Bill, Summary of the virtual workshop on the regulatory framework for online safety (18 June 2020).
[96] Government of Ireland, General Scheme of the Online Safety and Media Regulation Bill Q&A 7.
[97] ibid.
[98] General Scheme of the Online Safety and Media Regulation Bill, Head 55 (2).
[99] ibid Head 55 (5).
[100] ibid Head 55 (7).

explanatory note to this head of the General Scheme explains that this provided for the voluntary extra-jurisdictional application of the regulatory regime for online safety while respecting the practical and constitutional limitations of such application. However, these voluntary arrangements may not be successful in the removal of all reported cases of harmful online content such as intimate images hosted overseas. As a result, the intermediary goal of reducing visibility explained in section 5.2.6 would not be adequately addressed in many cases. However, this approach in Ireland is vital in establishing international collaborative channels and has the potential to result in greater compliance levels in the future.

5.3.6 The importance of transparency

It was highlighted in Chapter 3 that the Australian OESC lacks transparency in its decision-making process on what material meets the definition of 'intimate image',[101] 'cyberbullying material'[102] or 'prohibited content'.[103] In particular there is a lack of information around the OESC 'fact-finding steps' and the 'standard of proof' that they work under. It was suggested in Chapter 3 by 'Alannah & Madeline Foundation representative 1' that legislation in place at the time (Enhancing Online Safety Act 2015) required clearer definitions of what content is required to be removed by law so to provide clear standards upon which the efficiency of the eSafety Commissioner's decision-making processes for removal could be assessed. The provision of clearer definitions would provide greater foreseeability and would assist in the development of transparent removal procedures ensuring that content removed meets an established threshold therefore ensuring transparency and due process.

Similar to Australia, the Irish response needs to set a requirement in the legislation for clear transparency in how the OSC will assess the effectiveness of a platform's reporting mechanism and whether or not it is satisfying the online safety codes. The law needs to require the OSC to clearly show how they come to certain decisions. This would provide greater guidance to both the OSC in the exercise of their functions and further clarity for stakeholders in general.[104]

[101] Enhancing Online Safety Act 2015, s 9B as amended by the Enhancing Online Safety (Non-consensual sharing of intimate images) Act 2018.
[102] Enhancing Online Safety Act 2015, s 5.
[103] Broadcasting Services Act 1992, Schedule 7 clause 20 & 21.
[104] Government of Ireland, Online Safety and Media Regulation Bill, Summary of the virtual workshop on the regulatory framework for online safety (18 June 2020) 29.

5.3.7 Visibility

Chapter 3 identified a low level of awareness of the Australian OESC and that it would benefit from greater visibility. There is a need for people to know about such a body without having a specific reason for looking for it. Chapter 3 highlighted that the eSafety Commissioner's visibility is mainly with stakeholders in the technology industry or with people who engage in online regulation. However, there is a lack of visibility of the eSafety Commissioner in schools and with young people. A potential reason for this is that the eSafety Commissioner is a federal body and there tends to be a lack of awareness for federal bodies in general within Australia and more of an awareness for support provided at state/territory level. While this may not be an issue for Ireland due to its non-federal structure, there still needs to be an emphasis put on the promotion of the OSC so to ensure its visibility among the general public. Awareness workshops to be held in schools and national advertisement campaigns would be particularly helpful.

5.3.8 Independence

Both the OESC and the OSC sit within a larger governing body (Australian Communications and Media Authority and the Australian OESC and Media Commission respectively).

The question which arises is whether the OSC should follow the Australian approach and remain part of the Media Commission or whether Ireland should separate the OSC and establish it as its own separate entity. Research conducted in Chapter 3 highlighted a view that the OESC should be a separate entity from the ACMA.[105] This view was justified as it was highlighted that there are tensions between the OESC and the ACMA due to resourcing, budget decisions and responsibility. As a result, these issues cause tensions between member of both bodies. This issue may potentially arise within the Irish context due to the lack of clear guidance in the legislation over the structure and functions of the

[105] Interview with 'Anonymous interviewee 1' (Melbourne, 2019) and Interview with 'Anonymous interviewee 2' (Melbourne, 2019). See Chapter 3 section 3.6.5.4. 'The decision to make it its own entity. I wonder whether that is something that would be worth revisiting because so many of these issues do overlap . . . If you establish it as its own separate entity, then I think it would be useful to think very deeply about how that body can operate most effectively with other bodies that exercise similar sorts of functions and powers and responsibilities like violence and human rights issues'. ('Anonymous interviewee 1'); 'I don't think that's necessarily a happy relationship. I think there are a lot of interdepartmental tensions between the ACMA, the department and the eSafety Commissioner. And I think that manifests around resourcing and budget decisions as well as growing responsibility for other things. ('Anonymous interviewee 2').

Office. Considering the Australian approach has clear functions and powers set out for the OESC yet issues over responsibility and powers still arise, there is a strong potential these issues would arise in the Irish context due to the lack of legislative guidance. In particular, the Irish approach does not clearly set out the functions of the OSC and this could undermine its authority. While the Irish approach allows the Media Commission to delegate functions to various Commissioners including the OSC such as the ability to conduct an investigation, it cannot delegate functions in relation to sanctions. As a result, there is a clear argument for separating the OSC from the Media Commission and providing the OSC with their own budgeting and enforcement powers.

Another issue raised in the Australian context was whether the OESC would be best placed as a single entity or combined with another body. An argument put forward in favour of the OESC being a single entity was that many online safety issues overlap with the work of other organisations and sometimes it is better to look at issues through a broader outlook i.e. through an organisation who is equipped to considered multiple issues. In contrast to the argument in support of the Australian OESC becoming a single entity was that the OESC could become overloaded if it was to be the only stakeholder dealing with online safety issues. However, this argument was rebutted with the point that the OESC could sustain as a single entity so long as it continues to foster good relationships with other bodies in similar areas so that it can work effectively with these bodies when needed.[106]

The Australian experience has shown that the OESC should sit as an independent body so to avoid clashes in funding, allocation of resources, clashes in authority, and overlapping of processes. However, the research conducted above also highlighted that a single body may become overloaded and may have a broader view if linked to other organisations already in the field of online regulation. Therefore, Ireland must consider clarifying the specific authority and special role of the OSC and separate the OSC as an independent Commissioner from the Media Commission (who already is dealing with a wide array of issues). The OSC should be established as an independent separate entity with its own funding and resourcing and with the scope to deal with all areas of online safety but with the option to collaborate with other organisations as required. Importantly, the OSC should have the power to make decisions regarding administrative fines. The OSC as a single entity must be sufficiently resourced and funded unlike the experience

[106] See Chapter 3 section 3.6.5.4.

of the Data protection Commissioner in Ireland which has experienced significant challenges in accurately carrying out its functions due to the need for more staff and funding.[107] The funding for the Data Protection Commissioner has continued to increase over the last nine years from 1.9 million in 2014 to 23.2 million in 2022 so to more sufficiently equip this body.[108] In particular, similar to the OESC, the Data Protection Commissioner required additional funding so to develop a more robust ICT infrastructure to handle complaints and other issues.[109] The Irish government will need to consider equipping the OSC with adequate resources and funding from the outset as the lack of ability to carry out its functions effectively will be detrimental in its ability to remedy victims of IBSA and also to avoid the challenges and pitfalls in the context of funding which have been experienced by the Data Protection Commissioner and OESC.

5.4 Pre-legislative scrutiny of the General Scheme of the Online Safety and Media Regulation Bill

The Joint Committee on Tourism, Culture, Arts, Sport and Media undertook pre-legislative scrutiny of the General Scheme of the Online Safety and Media Regulation Bill in early February 2021.[110] The Joint Committee on Tourism, Culture, Arts, Sport and Media received written submissions from 61 stakeholders and held 15 oral hearings to consider pre-legislative scrutiny of the General Scheme of the Bill.[111] In November 2021, the Joint Committee on Tourism, Culture, Arts, Sport and Media published a report highlighting the core issues raised by stakeholders who presented evidence to the Committee in oral and written format and made 33 recommendations to be

---

[107] Ken Foxe, 'Revealed: Data Protection Commission's pleas for more staff and 'fit-for-purpose' office; (The Journal, 12th October 2019) < https://www.thejournal.ie/data-protection-budget-4848807-Oct2019/ > accessed 21 February 2022.

[108] Data Protection Commissioner, 'Data Protection Commission Statement on Budget 2022' (DPC, 12 October 2021) < https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-statement-budget-2022#:~:text=Commissioner%20Helen%20Dixon%20welcomes%20the,the%20Government%20in%20Budget%202022. > accessed 21 February 2022.

[109] Data Protection Commissioner, 'Data Protection Commission statement on funding in 2021 Budget' (DPC, 13 October 2020) < https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-statement-funding-2021-budget > accessed 21 February 2022.

[110] Houses of the Oireachtas, 'Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht seeks stakeholder and expert submissions on Online Safety and Media Regulation Bill 2020' (11 February 2021) < https://www.oireachtas.ie/en/press-centre/press-releases/20210211-joint-committee-on-media-tourism-arts-culture-sport-and-the-gaeltacht-seeks-stakeholder-and-expert-submissions-on-online-safety-and-media-regulation-bill-2020/ > accessed 22 February 2022.

[111] Joint Committee on Tourism, Culture, Arts, Sport and Media, *Report of the Joint Committee on the Pre-Legislative Scrutiny of the General Scheme of the Online Safety and Media Regulation Bill* (TCASM/21/07 — November 2021) Appendix 1 & 2.

included/amended in the General Scheme of the Bill/ adopted in Bill when initiated. In the context of this thesis, four recommendations were particularly relevant:

> 4. The Committee recommends that provisions be made for an individual complaints scheme within the General Scheme of the Bill
> 5. The Committee recommends that, where provisions are made for an individual complaints scheme, these provisions be responsive to the needs and protection of children and other vulnerable groups, and that these include effective takedown procedures and other appropriate measures.
> 14. The Committee recommends that Head 19 of the General Scheme of the Bill is amended to include the position of the Online Safety Commissioner.
> 20. The Committee recommends that highly precise detail is given as to the roles and responsibilities of the Media Commission and of the Online Safety Commissioner.[112]

The recommendations made in the report are discussed below. Whether the recommendations support the author's analysis of the General Scheme of the Bill in line with applied lessons learned from the author's study of the Australian context is considered.

5.4.1 The need for an individual complaints mechanism

The report highlighted a mixed view from stakeholders over whether the General Scheme of the Bill should include an individual complaints mechanism instead of or in addition to a systemic approach. It appears, however, that opposition to an individual complaints mechanism was primarily based on industry concerns. In particular, Facebook, Technology Ireland, and Twitter all strongly argued that such a system would be overwhelmed with complaints and therefore 'ineffective and administratively unworkable'.[113] However, the majority of stakeholders who engaged with the Joint Committee including the Ombudsman for Children's Office; Institute for Future Media; Democracy and Society; Child's Rights Alliance; the Australian eSafety Commissioner, Julie Inman Grant; Rape Crisis Network Ireland; Safe Ireland; Safety Over Stigma; Data Protection Commission; and CyberSafe Kids all highlighted that the lack of an individual complaints mechanism was a significant weakness within the Bill.

Similar to the suggestion under sections 4.6.2 as informed by the desk-based analyses of the OESC annual reports conducted in Chapter 2, the Irish Society for the Prevention of Cruelty to Children noted that concerns around complaint volume could be 'allayed'[114]

[112] ibid 11, 14.
[113] Joint Committee on Tourism, Culture, Arts, Sport and Media, *Report of the Joint Committee on the Pre-Legislative Scrutiny of the General Scheme of the Online Safety and Media Regulation Bill* (TCASM/21/07 — November 2021) 26.
[114] ibid 27.

by examining the functioning of the OESC. The OESC has had to manage individual complaints mechanisms across a wider span of reporting mechanisms including the IBA portal, the Cyberbullying Complaints Scheme and the Online Content Scheme. As noted in Chapter 2 the increased criminalisation of IBSA in Australia has not been a panacea for the challenge of IBSA. Issues around anonymity coupled with jurisdictional challenges, and issues with law enforcement investigative resources and lack of training have all hindered the effective combating of IBSA and highlighted the need for supplementary measures. In particular, a need for a specialist body, with expertise in internet regulation and a mandate in the area of IBSA was identified. A key response of the Australian system to the challenge of IBSA was the development of the OESC IBA portal which provides an individual complaints mechanism for victims of IBSA. While IBSA victims in Ireland may report their case to An Garda Síochána, it is envisaged that similar police challenges to those which create barriers for redress in Australia will be experienced in Ireland therefore there is a great need for an individual complaints mechanism as supported by the Joint Committee's report.

5.4.2 The functions of the Media Commission and establishment of an Online Safety Commissioner

A key finding of the interviews discussed in Chapter 3 was the benefit of clear avenues for collaboration and cooperation between the OESC and other organisations in assisting in the removal of harmful content.[115] The Joint Committee report highlighted how there needs to be clear guidance within the legislation for the role of the Media Commission but also its role in collaborating with other organisations. This was particularly highlighted by An Garda Síochána specifically suggesting that a memorandum of understanding be included within the legislation in order to ensure operational demands between An Garda Síochána and the Media Commission are appropriately managed.

In relation to the prospective work of the OSC specifically, the report highlighted that there was no explicit provision for the position of the OSC in Head 19 of the General Scheme of the Bill. This lack of precision in detailing the specific roles and responsibilities of the OSC could lead to challenges in the undertaking of their functions. The functions and powers of the OESC have been clearly set out in the various pieces of governing legislation despite always being under the remit of the ACMA. This has been

[115] See Chapter 3, section 3.6.1 & 3.6.4.

vitally important as it allows the OESC to carry out its functions in accordance with clear authority. While the functions of the Media Commission are set out, it was considered that the lack of guidance for the OSC may hinder the effectiveness and development of the body.

5.5 The Online Safety and Media Regulation Bill 2022

On the 14th of January 2022, the OSMRB 2022 was published. It was subsequently initiated in Seanad Éireann on the 25th of January 2022 for consideration for enactment. Below is an overview of the Bill highlighting areas which have been amended as compared to the General Scheme of the Bill in the context of IBSA. Overall, the Bill as initiated in the context of online safety follows the various Heads as set out under the General Scheme of the Bill. The initiated Bill provided the Coimisiún na Meán with the ability to audit complaints-handling processes,[116] issue guidance materials and advisory notices,[117] provide a scheme for notifications by nominated bodies,[118] and a duty to encourage the use of mediation between users and providers to resolve any dispute arising from users' complaints,[119] all in the same manner as the General Scheme of the Bill as outlined in Chapter 4 section 4.4.

The two main recommendations of the pre-legislative scrutiny of the Bill to include an individual complaints scheme and to clearly set out the functions and powers of the OSC were not included. However, on the 12th of January 2022, the leading Minister behind the Bill – the Minister of Tourism, Culture, Arts, Gaeltacht, Sport and Media, Catherine Martin – announced that an expert group led by Isolde Goggin[120] would assess within 90 days the practical possibility of including an individual complaints mechanism in the Bill.[121] Minister Martin committed to take the recommendations of the expert group into account when considering amendments to the Bill at Committee stage.

---

[116] The Online Safety and Media Regulation Bill 2022, s 139P.
[117] ibid s 139R, 139S.
[118] ibid s 139U.
[119] ibid s 139V.
[120] Chairperson, Competition and Consumer Protection Commission. The other members of the expert group are Brian O'Neill (Deputy Chair of the National Advisory Council for Online Safety), Ana Niculescu (CEO of Hotline.ie), Ronan Lupton (Senior Counsel), Baroness Kidron (Chair of 5Rights Foundation), Peter Tyndall (Information Commissioner).
[121] Government of Ireland, *Expert Group on an online safety individual complaints mechanism*, Terms of reference; Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media , 'Publication of Online Safety and Media Regulation Bill '(12 January 2022) < https://www.gov.ie/en/speech/a175a-publication-of-online-safety-and-media-regulation-bill/> accessed 24th January 2022.

Unlike the General Scheme of the Bill which referred to this regulatory body as the 'Media Commission', the Bill as initiated referred to the Media Commission as 'Coimisiún na Meán' or 'Commission' throughout the various sections of the Bill. The Bill followed the structure as set out in the General Scheme where Coimisiún na Meán was to be established as an independent regulatory body with similar functions and powers provided for under Section 7 of the Bill as initiated. Section 8 was designed to allow Coimisiún na Meán to delegate the performance of its functions to an individual Commissioner such as an OSC except in relation to the provision of sanctions.

While the General Scheme provided a definition of categories of harmful content, the initiated Bill provided a more exhaustive definition as follows:

> 139A.(1) For the purposes of this Act, online content is 'harmful online content' if it is one of the following 2 kinds:
>
> (a) content that falls within one of the offence-specific categories of online content defined in subsection (2);
>
> (b) content that—
>
> (i) falls within one of the other categories of online content defined in subsection (3), and
>
> (ii) meets the risk test defined in subsection (4).
>
> (2) The offence-specific categories of online content are—
>
> (a) the categories listed in Schedule 3, and
>
> (b) any category specified for the purposes of this paragraph by order under section 139B.
>
> (3) The other categories of online content are:
>
> (a) online content by which a person bullies or humiliates another person;
>
> (b) online content by which a person promotes or encourages behaviour that characterises a feeding or eating disorder;
>
> (c) online content by which a person promotes or encourages self-harm or suicide;
>
> (d) online content by which a person makes available knowledge of methods of self-harm or suicide;
>
> (e) any category specified for the purposes of this paragraph by order under section 139B.
>
> (4) Online content meets the risk test for the purposes of subsection (1)(b)
>
> (ii) if it gives rise to—
>
> (a) any risk to a person's life, or
>
> (b) a risk of significant harm to a person's physical or mental health,
>
> where the harm is reasonably foreseeable.
>
> (5) For the purposes of this Act, any question whether particular online content falls within a category under this section shall be determined on the balance of probabilities.

Similar to the General Scheme, Section 139A provided for the categories of online content that would fall under the definition of harmful online content, with the first category relating to offence-specific online content. Unlike the General Scheme which did not clearly outline the scope of content, which is a criminal offence to disseminate, the initiated Bill under Section 45 clearly set out each Act governed under Section 139(1)(a) and also mentioned the specific categories of content under each of these Acts. In particular, Section 45 clearly identified the Harassment Communications and Related Offences Act with specific reference to IBSA. The relevant subsections of Section 45 states:

> Harassment, Harmful Communications and Related Offences Act 2020
>
> 36. Online content by which a person distributes or publishes or threatens to distribute or publish an intimate image, contrary to section 2(1) of the Harassment, Harmful Communications and Related Offences Act 2020 (distribution etc. of image without consent and with intent to cause harm etc.).
>
> 37. Online content by which a person distributes or publishes an intimate image, contrary to section 3(1) of the Harassment, Harmful Communications and Related Offences Act 2020 (distribution etc. of image without consent and so as seriously to interfere with peace and privacy or to cause alarm, distress or harm).[122]

This change is significant in the context of IBSA as it clearly identifies IBSA as falling under the definition of the various categories of harmful content. It also makes it clear to potential victims that they may seek a remedy and support from Coimisiún na Meán/OSC. Although, due to the general nature of the legislation and broad array of offences included in the scope of the definition of harmful content, it seems clear that a strong communication strategy is important to make the general public aware of the implications of the law in the IBSA context.

Similar to Head 56 of the General Scheme of the Bill, Section 139E provided that Coimisiún na Meán would have the authority to designate a relevant online service as a service to which Online Safety Codes may be applied. Under Section 139E, the Commission would serve notice of a designation in relation to 'a named service, or in relation to all services falling within a category of services' described in the designation. In deciding whether or not to designate a service, the Commission would have regard to

[122] Online Safety and Media Regulation Bill 2022, s 45.

a number of matters, including the nature and scale of the service and the levels of risk of exposure to harmful online content when using the service. The initiated Bill maintained the provision of a system heavily based on Online Safety Codes to be drafted by Coimisiún na Meán and to be applicable to designated online services. The intention was that the online codes would operate on a systemic level by requiring designated services to operate in accordance with the codes and thus minimise the availability of harmful online content and protect users from harmful online content. The explanatory memorandum to the Bill stated that codes may also provide for:

> standards that services must meet, practices that providers must follow or measures that providers must take, standards, practices or measures relating to the moderation of content or how content is delivered, the assessment by service providers of the availability of harmful online content on services, of the risk of it being available, and of the risk posed to users by harmful online content, the making of reports by service providers to the Commission, and the handling by service providers of communications from users raising complaints. [123]

Section 139O provided that the Commission would by notice be able to require information from a provider of a designated online service relating to the compliance of the provider with an online safety code. Furthermore, Section 139P provided that the Commission would be able to appoint an independent person to carry out an audit of a designated online service's complaints and complaints-handling process in order for the Commission to assess compliance with an online safety code. The Commission would also be able to require by notice in writing the provider of a designated online service to co-operate with the person appointed to carry out the audit. Section 139Q provided that a failure to comply with an online safety code would result in a contravention and sanction.

5.6 Application of the victim-centred framework to the Irish situation

The insights gained from the desk-based research discussed in Chapter 2 and the interviews discussed in Chapter 3 on the functioning of the OESC in practice inform the analysis of the Irish approach. The victim-centred framework derived from the research conducted in the earlier chapters of this thesis incorporates these findings and insights gained from examining the policy and legislative history of this topic in Ireland. Chapter 4 applied the refined victim-centred framework developed from Chapter 3 to assess to what extent the Irish situation prior to the introduction of the OSMRA met the identified

[123] Online Safety and Media Regulation Bill 2022, Explanatory Memorandum.

victim needs. Results from this discussion are displayed in the refined table below as developed in Chapter 4.

Identified tools/mechanisms that address the needs of victims of IBSA

Identified needs of victims of IBSA	*Independent specialist authority*	*Individual complaints mechanism*	*Removal orders*	*Orders reducing visibility of IBSA material*	*Statutorily supported codes of practice*	*Educational campaigns*	*Civil avenues of redress*	*IBSA recognition as a criminal offence*
Constraining distribution of the image		Hotline.ie (limited powers and authority)[124]					Civil remedies, including damages and injunctive relief available	Harassment, Harmful Communications and Related Offences Act 2020, s 2 & s 3
Effective alternatives to constraining IBSA images								
Adequately trained and resourced authorities		Hotline.ie (limited powers and authority)[125]				Action Plan for Online Safety 2018/2019 – Action 1-5, 8, 9		
Prompt action		Hotline.ie (limited powers and authority)[126]						
Empowerment		Hotline.ie (limited powers and authority)[127]				Action Plan for Online Safety 2018/2019 – Action 1-5, 8, 9		Harassment, Harmful Communications and Related Offences Act 2020, s 2 & s 3
Confidentiality								Harassment, Harmful Communications and Related Offences Act 2020, s 5

Figure 16 Framework table of key needs and identified tools/mechanisms applied in the Irish context prior to the enactment of the Online Safety and Media Regulation Act 2022 as developed in Chapter 4

[124] Hotline.ie is a non-profit national reporting mechanism whereby members of the public can report concerns in respect of illegal content online. It has the power to inform service providers of the existence of suspected IBSA on their platform who may voluntarily remove the material as a result. They also refer suspected IBSA to An Garda Síochána.
[125] ibid.
[126] ibid.
[127] ibid.

Having set out the key components of the OSMRB as initiated, it is now necessary to consider the extent to which the approach put forward in the Bill had the potential to address the needs of victims of IBSA. The following sections will consider each identified victim need and to what extent each need could have been addressed by the OSMRB as initiated.

5.6.1 Constraining distribution of the image

In addition to the three tools/mechanisms[128] discussed in Chapter 4 which address the need of victims to constrain the distribution of their intimate images, this need can also be addressed through an independent specialist authority, statutorily supported codes of practice, and a systemic complaint scheme.

As previously discussed, the OSMRB 2022, as initiated, provided for the establishment of an independent specialist authority, An Coimisiún na Meán. As found in Chapter 2,[129] the research literature indicates that the appointment of an independent specialist authority with adequate powers can assist with the constraining of IBSA material distribution in a variety of ways.

As the OSMRB 2022 adopted a systemic approach to online safety, its primary intention was to constrain the distribution of harmful content at a system level as opposed to at an individual level. A key part of this approach is the provision made for binding Online Safety Codes that will apply to designated online services. While the Bill did not set out the Online Safety Codes (the Commission has responsibility for these) supporting documentation stated that the Online Safety Codes would include measures for online services to take to tackle the availability of harmful online content on their services, user complaint and/or issues handling mechanisms operated by online services, and risk and impact assessments for online services to take in relation to the availability of harmful online content on their services.[130] Extensive provision was made for investigative powers designed to investigate compliance and support enforcement of the codes.[131] Notably, section 139P provided for Coimisiún na Meán (or assuming delegation, the OSC) to audit the complaint handling services of online service providers to ensure that they meet the

[128] Individual complaints mechanism (Hotline.ie), civil avenues of redress, IBSA recognition as a criminal offence (Harassment, Harmful Communications and Related Offences Act 2020, s 2 and s 3).
[129] See Chapter 2 section 2.9.1.
[130] General Scheme of the Online Safety and Media Regulation Bill Head 50 (2); Government of Ireland, General Scheme of the Online Safety and Media Regulation Bill Q&A.
[131] Online Safety and Media Regulation Bill 2022, s 139O, s 139P and s 139Q.

required standards as established in Online Safety Codes. The conducting of these audits would allow shortcomings in these systems to be exposed and rectified thus making the complaints handling processes of online platforms more effective at achieving the constraining of IBSA material distribution. The OSMRB was designed to empower the Commission to impose financial sanctions where a designated online service provider failed to comply with an online safety code.[132] Moreover, notices to end contraventions, access blocking orders and content limitation notices were also provided for as important enforcement tools for the Commission.[133]

The 'scheme for notifications by nominated bodies' would provide a 'super-complaints' process that constitutes an important means by which systemic issues that perpetuate the distribution of IBSA material can be brought to the attention of the OSC.[134] Under this implementation of a systemic complaints scheme, 'nominated bodies' such as 'expert charities' are able to highlight systemic issues with relevant online services and designated online services to Coimisiún na Meán/OSC. The 'nominated bodies' can notify Coimisiún na Meán/OSC about issues relating to online service providers compliance with safety codes or for example the availability of harmful content such as IBSA on their platform. This can lead to An Coimisiún na Meán issuing proceedings to ensure the removal of content which in turn addresses the identified victim need of constraining the distribution of IBSA images. However, the nature of the systemic complaint system can be described as 'system-oriented'[135] rather than 'person-centred'[136] as the focus of this scheme is to provide an avenue to complain about service providers' systems or lack of compliance with safety codes. It does not provide for complaints about individual pieces of harmful content.

Chapter 2 also demonstrated the important educative role that can be played by a specialist authority and the OSMRB assigned some educative functions to the Commission – although not to the OSC in particular – under section 7(3)(f) stating:

> (3) Without prejudice to the generality of subsection (2), the Commission shall—
> (f) encourage research, promote or endorse educational initiatives and activities and co-operate for that purpose with educational bodies, and otherwise promote

[132] Online Safety and Media Regulation Bill, s. 139Q.
[133]ibid, s 139ZU and s139ZV.
[134] Online Safety and Media Regulation Bill, s139U.
[135] Ombudsman for Children, General Scheme of the Online Safety and Media Regulation Bill 2020, Submission by the Ombudsman for Children's Office to the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht (4 March 2021).
[136] ibid.

public awareness, knowledge and understanding, in relation to matters connected to its functions[137]

Such functions would ideally provide victims with knowledge on the harms of IBSA, where to seek help, and the options available to them in seeking removal. However, the Children's Rights Alliance, the Ombudsman for Children, and Women's Aid highlighted the lack of clarity within the Bill on the proposed awareness raising and education functions of the Commission, including with regard to online safety.[138]

5.6.2 Effective alternatives to constraining IBSA images

The identified need for effective alternatives to constraining IBSA images had the potential to be addressed through two of the noted tools/mechanisms in the OSMRB: an independent specialist authority and orders resulting from a contravention of the statutorily supported codes of conduct.

As discussed in Chapter 2, the complete removal of IBSA material may not always be possible and as a result the need for practical alternative solutions and effective remedies is necessary including 'recurring support and advice' for victims as they live with the 'ongoing fear that the images will re-emerge and continue to be re-shared'[139] and solutions designed to reduce the visibility of IBSA material on the internet.

The Irish statutory authority, Coimisiún na Meán and the OSC as provided for in the OSMRB had the potential to provide support, advice, education and awareness raising. The educative provisions have remained largely unchanged in the final text and the since established Coimisiún na Meán has launched a website (www.cnam.ie) which is envisaged to provide useful resources and support to victims. However, it is yet to be determined to what extent this website will be utilised and resourced. Children's Rights Alliance, the Ombudsman for Children, and Women's Aid highlighted that the Bill 'appears to be otherwise silent' on the proposed awareness raising and education

[137] Online Safety and Media Regulation Bill, s 7(3)(f).
[138] Children's Rights Alliance, Submission to the Joint Oireachtas Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht on the General Scheme of the Online Safety and Media Regulation Bill (8 March 2021); Ombudsman for Children, General Scheme of the Online Safety and Media Regulation Bill 2020, Submission by the Ombudsman for Children's Office to the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht (4 March 2021); Women's Aid, Submission to the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht on the General Scheme of the Online Safety and Media Regulation Bill (March 2021).
[139] Anastasia Powell, Asher Flynn, Adrian J. Scott and Nicola Henry, 'Image-Based Sexual Abuse: An International Study of Victims and Perpetrators' (Summary Report, February 2020)12.

functions of the Commission, including with regard to online safety.[140] As a result, it is unclear to what extent the provision of an independent statutory authority (Coimisiún na Meán) will address victims need for alternative solutions to the constraining of IBSA images.

As highlighted in Chapter 2, the scale and magnitude of the internet and the rapid spread of information make the constraining of intimate images challenging. As a result, reducing the visibility of IBSA is an important secondary measure. The OSMRB as initiated provided for orders limiting access to harmful content under section 139ZV such as intimate images and orders blocking access to certain harmful material within Ireland under section 139ZU. Such a provision would be particularly helpful where content is hosted overseas and/or where a designated service provider fails to adhere to online safety codes. This had the potential to address the need of IBSA victims for an effective alternative solution by reducing the visibility of IBSA material where removal is impossible. However, these orders were designed to only be issued in response to systemic issues rather than issues on an individual level.

5.6.3 Adequately trained and resourced authorities

In addition to the tool/mechanism of education campaigns discussed in Chapter 4 which partially addresses the need of victims for adequately trained and resourced authorities, the tool/mechanism of an independent statutory authority also addresses this need.

As discussed in Chapter 2, the academic literature demonstrates how the needs of victims have often been left unmet by under-trained and under-resourced authorities. In the Irish context, research carried out by Women's Aid on intimate relationships found that young people in Ireland are reluctant to raise online abuse issues and are reluctant to seek support through traditional avenues of redress.[141] As a result, a trained and resourced authority such as an independent specialist authority with a mandate to support victims of IBSA is vital. Coimisiún na Meán and the OSC in particular have the potential to address the need

[140] Children's Rights Alliance, Submission to the Joint Oireachtas Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht on the General Scheme of the Online Safety and Media Regulation Bill (8 March 2021); Ombudsman for Children, General Scheme of the Online Safety and Media Regulation Bill 2020, Submission by the Ombudsman for Children's Office to the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht (4 March 2021); Women's Aid, Submission to the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht on the General Scheme of the Online Safety and Media Regulation Bill (March 2021).

[141] Women's Aid, *One in Five Women Report, Experience Intimate Relationship Abuse Women's Aid 2020, TOO INTO you.*

of victims for an adequately trained and resourced authority as the OSC role is specifically designed to ensure online safety. In addition, Coimisiún na Meán is empowered with the ability to issue notices to end contraventions of Online Safety Codes and to take enforcement action through financial sanctions where needed. These tools are essential resources in tackling IBSA. As a result, the presence of such an authority equipped with statutory power addresses victims needs for an authority capable of effectively combatting IBSA. Furthermore, Coimisiún na Meán is envisaged to act as a key point of contact to liaise with other organisations such as An Garda Síochána and Hotline.ie in order to engage in knowledge exchange and the sharing of resources. However, it is yet to be determined to what extent Coimisiún na Meán will be funded, what level of resources it will receive, and to what extent it will engage with other organisations in order to address this need.

5.6.4 Prompt Action

As discussed in Chapter 4, the individual complaint mechanism administered by Hotline.ie provides prompt access to a potential avenue of removal for victims of IBSA. Although it is notably less powerful than the Australian IBA portal with no power to enforce removal requests or seek court assistance. It is also unclear whether the enforcement powers of Coimisiún na Meán — access blocking orders and content limitations orders — made in response to safety code violations under the OSMRB would address this victim need for prompt action. As a general point, the measures set out in the Bill are designed to address the issue of online harm at a systemic rather than an individual scale and thus the potential to meet the needs of individuals by way of direct prompt action is somewhat limited. In spite of this, however, action taken by the Commission in response to breaches of the online safety codes could result in more transparent and efficient complaint systems administered by the platforms, likely resulting in more prompt removal of IBSA content at a systemic level.

5.6.5 Empowerment

In addition to the three tools/mechanisms already discussed in Chapter 4 which address victims need for empowerment,[142] an independent statutory authority also has the potential to address this need.

As discussed in Chapter 2,[143] an independent specialist authority can empower victims by providing support, advice, and guidance enabling victims to regain control of their lives. Coimisiún na Meán has the potential to provide this support through educational tools and resources on their website (www.cnam.ie). The use of such services equips victims with options allowing them to make informed decisions on what avenue of redress is most suitable for their experience. It is yet to be determined if this authority will provide such support to empower victims.

As a direct point on empowerment, it is notable that the OSMRB did not provide for an individual complaints mechanism but instead provided for a systemic approach with a focus on Online Safety Codes and a 'super complaints' scheme for nominated bodies which would exclude victims from reporting directly to the OSC. This can be viewed as disempowering to victims as victims do not have direct access to the OSC and may accordingly feel locked-out and powerless.

5.6.6 Confidentiality

The tools/mechanisms discussed in this chapter that derived from the OSMRB are not pertinent to the need of victims of IBSA for confidentiality.

5.6.7 Assessing how the Online Safety and Media Regulation Bill as initiated had the potential to improve the Irish response to the needs of IBSA victims

The OSMRB was a positive step towards recognising the need for varied responses to the needs of victims of online harm. While some limited tools/mechanisms that partially responded to the needs of IBSA victims existed prior to the OSMRB, clear gaps in protection remained. The regulatory scheme set out in the OSMRB had the potential to respond to at least some of the identified victim needs. For example, the OSMRB recognised the importance of establishing a statutory body with authority in the area of online harms. One innovation of the OSMRB was the 'scheme for notifications by

[142] The tools/mechanisms discussed include: Individual complaints mechanism (Hotline.ie), Educational Campaigns (Action Plan for Online Safety 2018/2019 – Action 1-5, 8, 9), IBSA recognition as a criminal offence (Harassment, Harmful Communications and Related Offences Act 2020, s 2 & s 3.
[143] See Chapter 2 section 2.9.5.

nominated bodies' which was designed to function as a type of 'super-complaints' system. While a systemic complaints scheme may not address the same needs that are addressed by an individual complaints mechanism, the potential of such schemes to address victim needs at least in part is recognised by the insertion of a new tools/mechanisms column in the table below, 'Systemic complaint scheme'. The below table is updated to specifically identify the additional tools/mechanisms introduced by the OSMRB and highlights which victim needs these tools/mechanisms had the potential to address.

Identified tools/mechanisms that address the needs of victims of IBSA

Identified needs of victims of IBSA

	Independent specialist authority	*Individual complaints mechanism*	*Removal orders*	*Orders reducing visibility of IBSA material*	*Statutorily supported codes of practice*	*Systemic complaint scheme*	*Educational campaigns*	*Civil avenues of redress*	*IBSA recognition as a criminal offence*
Constraining distribution of the image	Coimisiún na Meán delegating powers to the Online Safety Commissioner – Online Safety and Media Regulation Bill 2022 as initiated, s 7& s 8	Hotline.ie (limited powers and authority)[144]			Online Safety Codes – Online Safety and Media Regulation Bill 2022 – s 139K Notice to end contravention - Online Safety and Media Regulation Bill 2022, s 139ZT	Systemic complaint scheme – Online Safety and Media Regulation Bill 2022, s 139U		Civil remedies, including damages and injunctive relief available	Harassment, Harmful Communications and Related Offences Act 2020, s 2 & s 3
Effective alternatives to constraining IBSA images	Coimisiún na Meán delegating powers to the Online Safety Commissioner – Online Safety and Media Regulation Bill 2022, s 7 & s 8				Access blocking order & Content limitation notice-Online Safety and Media Regulation Bill 2022, s 139ZU & s139ZV (resulting from contraventions of online safety codes)				
Adequately trained and resourced authorities	Coimisiún na Meán delegating powers to the Online Safety Commissioner – Online Safety and Media Regulation Bill 2022, s 7 & s 8	Hotline.ie (limited powers and authority)[145]					Action Plan for Online Safety 2018/2019 – Action 1-5, 8, 9		
Prompt action	Coimisiún na Meán delegating powers to the Online Safety Commissioner – Online Safety and Media Regulation Bill 2022, s 7 & s 8	Hotline.ie (limited powers and authority)[146]			Notice to end contravention - Online Safety and Media Regulation Bill 2022, s 139ZT				
Empowerment	Coimisiún na Meán delegating powers to the Online Safety Commissioner – Online Safety and Media Regulation Bill 2022, s 7 & s 8	Hotline.ie (limited powers and authority)[147]					Action Plan for Online Safety 2018/2019 – Action 1-5, 8, 9		Harassment, Harmful Communications and Related Offences Act 2020, s 2 & s 3

[144] Hotline.ie is a non-profit national reporting mechanism whereby members of the public can report concerns in respect of illegal content online. It has the power to inform service providers of the existence of suspected IBSA on their platform who may voluntarily remove the material as a result. They also refer suspected IBSA to An Garda Síochána.

[145] ibid.

[146] ibid.

[147] ibid.

Confidentiality									Harassment, Harmful Communications and Related Offences Act 2020, s 5

Figure 17 Framework table of key needs and identified tools/mechanisms applied in the Irish context incorporating the Online Safety and Media Regulation Bill

5.7 More recent updates: The Online Safety and Media Regulation Act 2022

Subsequent to the conducting of the initial research and analysis of this thesis, a report from the Expert Group on the feasibility of an individual complaints mechanism[148] was released and the OSMRA 2022 was enacted. The following sections will briefly outline these updates.

5.7.1 Expert Group Report

As noted in section 5.5, on the 12th of January 2022, the leading Minister behind the OSMRB – the Minister of Tourism, Culture, Arts, Gaeltacht, Sport and Media, Catherine Martin – announced that an expert group led by Isolde Goggin[149] would assess within 90 days the practical possibility of including an individual complaints mechanism in the Bill.[150] The expert group was tasked with examining whether 'an individual complaints mechanism is practicable in the context of the OSMRB and, if not, if there is another method of resolving matters raised by such a mechanism'.[151] The Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media called for submissions to be made to the Expert Group which opened on the 28th of February 2022 and ended on the 21st of March 2022. During the public consultation period, 20 submissions[152] were made which informed the

[148] An 'individual complaints mechanism' is defined as 'a mechanism whereby members of the public may complain to an Online Safety Commissioner about individual items of content that they suspect may fall within a category of harmful online content' Government of Ireland, *Expert Group on an online safety individual complaints mechanism*, Terms of reference.

[149] Chairperson, Competition and Consumer Protection Commission. The other members of the expert group are Brian O'Neill (Deputy Chair of the National Advisory Council for Online Safety), Ana Niculescu (CEO of Hotline.ie), Ronan Lupton (Senior Counsel), Baroness Kidron (Chair of 5Rights Foundation), Peter Tyndall (Information Commissioner).

[150] Government of Ireland, *Expert Group on an online safety individual complaints mechanism*, Terms of reference; Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media , 'Publication of Online Safety and Media Regulation Bill '(12 January 2022) < https://www.gov.ie/en/speech/a175a-publication-of-online-safety-and-media-regulation-bill/> accessed 24th January 2022.

[151] Government of Ireland, *Expert Group on an online safety individual complaints mechanism, Terms of reference*.

[152] The 20 submissions included: Dublin Rape Crisis Centre, Broadcasting Authority of Ireland, American Chamber of Commerce Ireland, Advertising Standards Authority for Ireland, CyberSafe Kids, DCU, Public Response, ISPCC, Law Society of Ireland, IAB Ireland, RTÉ, Meta, Ombudsman for Children, Caliber AI, RCNI, Extern, Childrens Rights Alliance, Technology Ireland, and Women's Aid.

final report. On the 20th of September 2022 the Minister for Tourism, Culture, Arts, Gaeltacht, Sport and Media, Catherine Martin, published the Report of the Expert Group on an Individual Complaints Mechanism.[153]

The expert group concluded that 'such a mechanism is feasible, subject to certain conditions being met'.[154] In particular, an individual complaints mechanism should not be viewed as a 'replacement for the online platforms' complaint handling processes' and it should be introduced on a 'phased basis', 'prioritising those complaints where the online content in question relates to children'.[155]

With regard to the structure and operation of an individual complaints mechanism the Report made a number of recommendations. Such recommendations include that an individual complaints mechanism should be structurally separate from the systemic regulatory functions of Coimisiún na Meán.[156] Furthermore the report also recommended that the Coimisiún na Meán be enabled to triage and refer complaints to certain other bodies, such as An Garda Síochána and Hotline.ie.[157] The report also recommended that a person making a complaint to the individual complaints mechanism must first have complained to the provider of the designated online service through which the alleged harmful online content is available and where either a) the complainant is unsatisfied with the provider's response, or b) an unreasonable period of time has elapsed without a response from the provider.[158]

Finally, the expert group's report sets out how the 'phased' implementation of an individual complaints mechanism should occur. The report recommends a four-stage approach including:

1. The development and application of relevant Online Safety Codes on complaints handling by Coimisiún na Meán;

2. The monitoring of the compliance of designated online services with the Online Safety Codes on complaints handling made by An Coimisiún over a period of at least 12 months;

---

[153] Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media, 'Expert Group Backs the Feasibility of an Individual Complaints Mechanism' (Press Release, 20 September 2022) < gov.ie - Expert Group backs the feasibility of an Individual Complaints Mechanism (www.gov.ie) > accessed 8th May 2023.
[154] Expert Group, *Report of the Expert Group on an Individual Complaints Mechanism* (May 2022) 1.
[155] ibid.
[156] ibid, 2.
[157] ibid.
[158] ibid, 3.

3. The development of an initial individual complaints scheme focused on one or more of the categories of non-offence specific harmful online content, for example: cyberbullying, where the online content pertains to a child; and

4. The development and publication of a work plan setting out how An Coimisiún shall work towards operating an individual complaints mechanism in full.[159]

5.7.2 Online Safety and Media Regulation Act 2022

The OSMRA 2022 was enacted on the 10th of December 2022. On the 22nd of February 2023, the Minister for Tourism, Culture, Arts, Gaeltacht, Sport and Media, Catherine Martin signed the Online Safety and Media Regulation Act (Commencement) Order 2023[160] establishing Coimisiún na Meán on an administrative basis with formal establishment commencing from 15 March 2023. Four Commissioners were formally appointed including Jeremy Godfrey as Executive Chairperson, Niamh Hodnett as Online Safety Commissioner, Rónán Ó Domhnaill as Media Development Commissioner, and Celene Craig as Broadcasting Commissioner. The Act largely follows the proposals as set out under the OSMRB 2022 with regard to:

- defining 'harmful online content'
- the making of binding online safety codes, which will tackle the availability of the categories of harmful online content by addressing a wide range of issues from content moderation to complaints handling
- the process for designating online services for regulation
- the making of non-binding online safety guidance materials and advisory notices to further create and support a safety-first culture of compliance
- the establishment of a 'super-complaints' scheme where nominated bodies, including expert NGOs in areas such as child protection, can bring systemic issues to the attention of Coimisiún na Meán

However, in addition, the Act introduces a legal basis for Coimisiún na Meán to establish individual complaints schemes allowing individuals to submit complaints about alleged harmful online content such as IBSA directly to the regulator. Part 11 Chapter 4 on the OSMRA governs 'Complaints to Commission about harmful online content'. Section 139V allows for Coimisiún na Meán to 'make a scheme relating to complaints about the

[159] Expert Group, *Report of the Expert Group on an Individual Complaints Mechanism* (May 2022) 3 & 4.
[160] S.I. No. 71/2023 - Online Safety and Media Regulation Act 2022 (Commencement) Order 2023

availability of a type of harmful online content on designated online services'.[161] Furthermore, such schemes, if introduced, will be governed by the procedures and subject to the requirements as set out under Part 11 Chapter 4.[162] Section 139S set out the conditions which must be met in order for an individual complaint to be considered under a scheme. The conditions under section 139S include:

> (a) the complainant has made a complaint to the provider of the designated online service concerned about the availability of the content on the service;
>
> (b) a period of more than 2 days has elapsed since the complainant made the complaint to the provider;

(c) where the provider operates a process in accordance with an online safety code for handling such a complaint, the complainant has taken reasonable steps in that period to have the complaint resolved through that process[163]

Resolutions to complaints provided for under section 139T of the Act include:

- referring the complaint to the provider concerned with such advice, guidance or support as the Commission considers appropriate
- bringing the complaint to the attention of another body such as An Garda Síochána or Hotline.ie
- issuing a content limitation notice as set out under section 139ZZD

Overall, while these new developments are a move in the right direction, it is yet to be determined if a complaints scheme will be set up for the reporting of IBSA. As a result, it is unknown to what extent the OSMRA 2022 will address the needs of victims in the context of IBSA beyond what the OSMR Bill had the potential to address if it had been enacted as initiated. Accordingly, the table below remains largely unchanged in light of the adoption of the OSMRA 2022, apart from updating the references to specific sections of the OSMRA 2022. Further research will be required, as/when Online Safety Codes are drafted and applied, and if/when relevant individual complaint schemes are established. This research would focus on evaluating to what extent any codes that are adopted and/or individual compliant scheme adopted address the needs of victims as identified in this thesis.

[161] Online Safety and Media Regulation Act 2022, s 139V. No individual complaints scheme has been introduced to date at the time of finalising this thesis.
[162] ibid, s 139R.
[163] ibid, s 139S.

Identified tools/mechanisms that address the needs of victims of IBSA

Identified needs of victims of IBSA

	Independent specialist authority	*Individual complaints mechanism*	*Removal orders*	*Orders reducing visibility of IBSA material*	*Statutorily supported codes of practice*	*Systemic complaint scheme*	*Educational campaigns*	*Civil avenues of redress*	*IBSA recognition as a criminal offence*
Constraining distribution of the image	Coimisiún na Meán delegating powers to the Online Safety Commissioner – Online Safety and Media Regulation Act 2022 as initiated, s 6& s 7	Hotline.ie (limited powers and authority)[164]			Online Safety Codes – Online Safety and Media Regulation Act 2022 – s 139K Notice to end contravention - Online Safety and Media Regulation Act 2022, s 139ZZB	Systemic complaint scheme – Online Safety and Media Regulation Act 2022, s 139ZC		Civil remedies, including damages and injunctive relief available	Harassment, Harmful Communications and Related Offences Act 2020, s 2 & s 3
Effective alternatives to constraining IBSA images	Coimisiún na Meán delegating powers to the Online Safety Commissioner – Online Safety and Media Regulation Act2022, s 6 & s 7				Access blocking order & Content limitation notice- Online Safety and Media Regulation Act 2022, s 139ZZC & s139ZZD (resulting from contraventions of online safety codes)				
Adequately trained and resourced authorities	Coimisiún na Meán delegating powers to the Online Safety Commissioner – Online Safety and Media Regulation Act 2022, s 6 & s 7	Hotline.ie (limited powers and authority)[165]					Action Plan for Online Safety 2018/2019 – Action 1-5, 8, 9		
Prompt action	Coimisiún na Meán delegating powers to the Online Safety Commissioner – Online Safety and Media Regulation Act 2022, s 6 & s 7	Hotline.ie (limited powers and authority)[166]			Notice to end contravention - Online Safety and Media Regulation Act 2022, s 139ZZB				
Empowerment	Coimisiún na Meán delegating powers to the Online Safety Commissioner – Online Safety and Media Regulation Act 2022, s 6 & s 7	Hotline.ie (limited powers and authority)[167]					Action Plan for Online Safety 2018/2019 – Action 1-5, 8, 9		Harassment, Harmful Communications and Related Offences Act 2020, s 2 & s 3

[164] Hotline.ie is a non-profit national reporting mechanism whereby members of the public can report concerns in respect of illegal content online. It has the power to inform service providers of the existence of suspected IBSA on their platform who may voluntarily remove the material as a result. They also refer suspected IBSA to An Garda Siochana.

[165] ibid.

[166] ibid.

[167] ibid.

Confidentiality									Harassment, Harmful Communications and Related Offences Act 2020, s 5

Figure 18 Framework table of key needs and identified tools/mechanisms applied in the Irish context incorporating the Online Safety and Media Regulation Act

However, the extent to which the approach will fulfil victim needs will be dependent on how this Act is applied in practice. Thus, ongoing/future research is necessary which this research hopes to inform.

5.8 Conclusion

While the criminalisation of IBSA was identified as a positive step for victims of IBSA in Ireland, even where the criminal process runs as intended, it only provides for the prosecution of the perpetrator. This is often a secondary priority of victims of IBSA, who often place most value on the removal of the images from the internet.[168] Furthermore the potential of re-traumatisation of victims during criminal proceedings and lengthy court processes highlighted the need for a supplementary avenue of complaint for victims. While a new body as discussed should not be seen as an alternative to adequate training and resourcing of law enforcement in the area of IBSA, the need for a dedicated body with expertise in the space of IBSA and the ability to provide an alternative model of complaint and redress for victims is clear. As identified within the Australian system, and as reflected in the new consolidated legislation, The Online Safety Act 2021, there is merit to a comprehensive approach to the regulation of harmful content such as IBSA on the internet instead of separate targeted pieces of legislation which can be piecemeal and complex when applied in practice.

The OESC started as a body designed to protect children but then needed to expand to cover all individuals resident in Australia. The incremental growth in OESC powers and scope meant that the OESC developed competence and expertise over time which resulted in the development of targeted reporting mechanisms and the creation of specified teams such as the IBA team to deal with such mechanisms. The Irish approach creates a new body 'Coimisiún na Meán' (amalgamating the Broadcasting Authority of Ireland) with a vastly increased set of powers and functions in the online space. 'Coimisiún na Meán'

[168] Nicola Henry, Asher Flynn & Anastasia Powell (2018) 19 Policing image-based sexual abuse: stakeholder perspectives, Police Practice and Research 565.

will maintain the current staff of the Broadcasting Authority of Ireland (BAI) while also recruiting additional staff. In spite of benefiting from the experience of the BAI, developing knowledge and expertise in the area of harmful online content will be a significant undertaking that will require high levels of resources and training. It could be argued that the gradual expansion of the OESC scope to include the area of IBSA by first enhancing its role in relation to education and research functions provided a sound basis for the subsequently granted enforcement powers. Expanding its scope of authority into those areas first also allowed the body to begin working in the area more quickly as the legislative process for statutory powers was underway. While it may have been desirable to have a dedicated body working in the IBSA educative and research space in Ireland before now, the urgency of the situation due to the increased number of IBSA incidences, supports the establishment of the Commission and the recent appointment of the OSC. The current priority is the allocation of extensive funding and recruitment for the OSC to ensure that the online safety mission is given the appropriate prominence and focus from the outset.

The OESC are required to release an annual report. Under the Australian legislation in place at the time of the interviews discussed in Chapter 3, there was no guidance on what information should be included in these reports. The Online Safety Act 2021 now requires the OESC to report on wide variety of matters with specific detail. For example, the OESC must report on the number of complaints made, the number of investigations conducted, and the number of notices issues. The requirement for specific details and statistics to be published is positive as it provides vital insight into the functioning of the organisation and helps the public to assess whether the body and law are operating effectively. While the Australian Online Safety Act 2021 requires some specific information to be included in the annual reports, it does not require information on investigation time frames. This would be a valuable additional data point which should be recorded and made publicly available as it provides insight into how quickly a report is responded to. While the OSMRA requires ‘Coimisiún na Meán’ to release an annual report, the OSRMA does not state what level of detail should be provided in the report. As a result, the author recommends the Irish legislation require the publication of detailed annual reports specifying what should be included in the report similar to the Australian context under the Online Safety Act but with the added requirement of the publication of timelines for investigations of complaints. These detailed reports will provide transparency as regards

to Coimisiún na Meán processes and actions. Such information will be vital in ensuring the effectiveness of the law and that the body can be kept under review.

The Australian OESC does not collect or publish information on whether harmful material such as intimate images reported to the OESC remains offline permanently (or even for an extended period) or whether victims experience revictimization through the material resurfacing on other platforms by either the original or new perpetrators. Understanding whether reported material remains offline once reported to the OESC would provide a better understanding as to whether victims of IBSA would be able to regain control of their intimate images. While tracking this is likely to be a challenging task, indeed an impossible task to achieve in every instance, a system for recording repeated infractions is necessary to provide insight into the true effectiveness of the system and to help identify where additional action may be needed. The Irish response must learn from this limitation of the OESC and ensure Coimisiún na Meán tracks the outcome of its cases over time and implements a system to facilitate this. The OESC engages extensively with a variety of stakeholders, including NGOs, legal practitioners, academics, online intermediaries, and technology industry bodies. Furthermore, the OESC fosters engagement through a wide variety of means including reference groups/committees, the trusted eSafety providers scheme, and commissioning research projects. The benefits of such engagement are greater cooperation, more knowledge exchange, increased awareness raising, and an expanded opportunity to connect with victims through referrals. It is important Ireland establishes clear avenues for stakeholders to engage with the OSC in the Irish context.

Research conducted illustrated the challenges facing the OESC when seeking to remove IBSA material from the internet due to the rapid speed at which online content spreads. This challenge is magnified further where issues related to jurisdiction and anonymity apply. The OESC particularly struggle to bring about the removal of harmful content hosted overseas. Furthermore, while the OESC has established strong cooperative relationships with the main online platforms and providers, problems still remain with smaller websites which can be more difficult to locate and are more likely to refuse to follow the direction of the OESC. As described in Chapter 3, the OESC response to these challenges is to request search engines to voluntarily de-index content in an effort to limit the accessibility of IBSA material and thus mitigate the harm for victims. If a request to de-list is not complied with, the Online Safety Act 2021 empowers the OESC to issue link deletion notices and app removal notices to direct a search engine provider or an app

store to remove a link or app which provides access to reported harmful material particularly in cases where the content is hosted overseas. The Irish response fails to provide for an alternative action (where the ultimate goal of complete removal is not possible) which is fast and conscious of human rights obligations. While Coimisiún na Meán can seek an order to block access to a service which fails to comply with a safety code or issue a content limitation notice to remove, disable access, or limit access to content which fails to comply with a safety code, such actions are taken at a systemic rather than an individual level and require an investigation and a court application.

While the Australian OESC process can be assessed as relatively streamlined compared to the Australian criminal justice process, the imposing of an enforcement action – including an injunction, enforceable undertaking or a civil penalty – requires a court order and this inevitably slows down the process. However, the OESC does have the option of issuing an infringement notice without a court order which can later be appealed to a court. As discussed in Chapter 3, Nicolas Suzor and Peter Clarke recommended that in order to effectively address the immediacy and scale of distribution in the online sphere, the regulator should be empowered to make a determination and issue all enforcement actions without a court order, but which can later be appealed to a court. The requirement under the Online Safety Act 2021 for the OESC to provide an internal review process would provide an additional safeguard and avenue to ensure due process if such an approach was taken. The Irish response requires lengthy investigative and court processes which will slow down the process of removing harmful content and as current proposals are designed to operate at the systemic level, gaps in protection are likely to arise. Certain features of the Australian system could be adopted to speed up the process. For example, it is likely that allowing the direct reporting by victims and individuals to the OESC, providing for infringement notices which do not require a court order, and mandating a 24-hour time frame for removal would lead to more timely removal in Ireland. The timely removal of content under the Irish proposals would be much more reliant on the operation of the service providers complaints mechanisms – presumably developed to align to the planned online safety codes. While the OSMRA 2022 allows for the establishment of individual complaint schemes, it is unclear whether a scheme will be established that applies to IBSA material. Even if such a scheme is eventually established, it will likely not be operational for several years. As a result, this thesis recommends a more empowered regulator, with a mandate to investigate individual instances of harm including IBSA specifically in addition to systemic risk. If a relevant individual

complaints scheme is established, this author would recommend that in the particular context of IBSA, the regulator should have the option to order the immediate takedown of suspected illegal content in line with clear safeguard measures and review processes. The service providers would retain the ability to appeal the decision in the courts. A similar process is already in practice in the Irish context through the Financial Services and Pensions Ombudsman whereby an individual can make a complaint if they are not satisfied with their dealings with a financial services firm or a pensions administrator. Following making a complaint to the Financial Services and Pensions Ombudsman, this authority can make a binding decision which can then be appealed to the High Court if either the individual or financial services firm or pensions administrator are unhappy with the decision. Therefore, the ability for a regulatory authority to make a legal determination which can later be appealed to a court is established within Ireland. The provision of an individual complaints mechanism by the OESC — which includes not only the ability to complain about an intimate image disseminated without consent but also the ability to object to an intimate image which was once consensual but where later consent was retracted — provides an alternative or supplementary avenue of complaint and redress for victims in addition to the criminal process or traditional civil approach. Criminal and civil approaches can be time consuming, costly and re-traumatising. Furthermore, the OESC provides an alternative route for victims who are unable to articulate their concerns to platforms or are struggling in their interactions with platforms. The OESC has greater impact than an individual when approaching a platform with a removal request. The Irish response currently fails to provide this support to victims and it is unclear whether an individual complaints mechanism will be implemented for victims of IBSA or whether the Irish response will follow the recommendations of the expert group and focus such a mechanism to only respond to online issues pertaining to children. With the lack of an individual complaints mechanism, the only option for victims in Ireland is to rely on the complaints handling systems of online platforms. As a result, the Irish system misses an opportunity to provide an invaluable and empowering tool for victims of IBSA seeking to reassert control over their image.

The OESC only removes the reported harmful content and not surrounding or associated content. This was confirmed by representatives of the OESC during interviews. The current Irish regulatory response, which adopts a purely systemic approach, leaves the decision about what content to be removed in individual cases to the service providers. It is essential that the Irish system provides clear guidelines about how such systems should

be implemented by services in accordance with strict removal procedures. It is interesting to note that there is provision made in the Irish Act for systemic complaints to be made by nominated bodies on the grounds of the infringement of rights, including freedom of expression.[169] This has the potential to be an important check on service providers who may be inclined to adopt a delete first policy to mitigate any risk of non-compliance.

Harsh penalties may create a system of uncertainty for social media providers. As a result, penalties must be backed by due process safeguards so to prevent the removal of legitimate content. Previously, in Australia there was a lack of safeguards under the legislation in place at the time of the interviews, however, the Australian Online Safety Act 2021 developed an internal review process which allows for a review of decisions made by the OESC. The Irish approach must ensure safeguards are in place alongside any penalty systems. An internal review process provides an example of such a safeguard. This will be particularly important if an individual complaints mechanism is introduced to include complaints about IBSA material.

While the OSMR Act makes progress in providing a regulatory system for online safety that tackles online harms including IBSA, the Irish response could be improved in order to better address the needs of victims. Developments in the drafting and application of the Online Safety Codes and their potential to foster a safer online environment will have to be monitored closely. While the challenges of implementing an individual complaints mechanism are acknowledged, the systemic approach is unlikely to fully address the needs of victims of IBSA as identified in this thesis. While it is positive that the possibility of an individual complaints mechanism has been provided for in the Act, it is yet to be determined whether such a scheme will be implemented in the IBSA context.

[169] Online Safety and Media Regulation Bill 2022, s 139U 3(d).

Chapter 6: Summary of major findings and key recommendations from a victim-centred perspective

1. Introduction

Image-based sexual abuse (IBSA) is a global issue that has increased in both prevalence and potential to cause harm in line with technological developments which have facilitated the taking, altering, and distribution of intimate images. Many jurisdictions have attempted to combat these behaviours through the implementation of targeted criminal laws and also, in some jurisdictions, by creating regulatory systems and establishing bodies with powers in the area. This thesis provides a comprehensive analysis of the Irish legislative response to IBSA by considering the history and drafting which led to the enactment of the OSMRA and analysing the potential of the nascent regulatory system for online safety to respond to the needs of victims of IBSA. A critical preliminary step necessary to inform this task was the analysis of a well-established regulatory response to online safety issues. The Australian system – with its Office of the eSafety Commissioner (OESC) – was the ideal comparator.

The analysis in this thesis is informed by a victim-centred perspective. In order to conduct the research from a victim-centred perspective, the key needs of victims of IBSA and the key mechanisms designed to address those needs, at least in part, were identified through desk-based research drawing from literature and interviews with key IBSA stakeholders. These findings formed the basis of the victim-centred framework developed and applied in this thesis. This framework, as set out in a table, facilitated the in-depth analysis of the Australian and Irish responses to IBSA. [1]

The extensive study of the Australian system revealed clear lessons applicable in the development and design of the Irish response to IBSA, most notably in relation to the operation of the Irish Online Safety Commissioner (OSC). Following the investigation carried out in this thesis, it is clear that the Irish regulatory response – as contained in the Online Safety and Media Regulation Act 2022 (OSMRA) – requires further improvement to ensure that the needs of victims are adequately addressed.

[1] See Chapter 2 section 2.9.

2. Chapter overview

Chapter 1 of this thesis aimed to define, examine, and discuss the key terms, concepts, and technologies referenced throughout the thesis in order to provide a foundation for later discussions and analysis. Chapter 1 relied on a desk-based analysis of existing literature relating to the concept and development of IBSA, the role of the internet in facilitating the perpetration of IBSA, specific legal issues raised in the online context and their impact on the regulation of IBSA, the development of laws criminalising IBSA, the role of intermediaries, and the rights of privacy and freedom of expression. Understanding the scope of IBSA and the impact of technology in facilitating it was crucial as it provided a basis for the arguments made in this thesis and highlighted the fact that while IBSA is not a new crime, its modern incarnation is inherently tied to the internet and the platforms that enable the distribution of such content. As a result, it was made clear that a key aim of any effective response to the harm caused by IBSA must be to combat this offence within the online sphere through the removal of IBSA content. Chapter 1 also demonstrated that social media platforms and pornography sites facilitate the spread of such images and as a result require particular attention when developing a regulatory response. Achieving a balance between the right to privacy and freedom of expression in the context of IBSA is complex. While Chapter 1 made it clear that the breach of a person's sexual privacy is at the core of an act of IBSA, Chapter 1 also highlighted that the over-regulation of content such as intimate images may lead to the removal of legitimate content which can have a chilling effect on freedom of expression. As a result, Chapter 1 highlighted how the consideration of safeguards and strict removal procedures when developing a regulatory response to IBSA is essential. Overall, the understanding of key terms, concepts, and technologies provided greater insight into the specific needs of IBSA victims and provided important context that assisted the assessment of which tools/mechanisms have the potential to respond effectively to the needs of victims. As a result, this insight informed the development of the victim-centred framework in later chapters.

Chapter 2 aimed to conduct a comprehensive assessment of the Australian response to IBSA from a victim-centred perspective. This chapter focused on examining the effectiveness of the Australian regulatory system and the OESC in practice through a desk-based analysis of key documents with particular attention afforded to the OESC annual reports and the Briggs report. This chapter aimed to identify the merits and

demerits of the regulatory system with a particular focus on the OESC and to inform the development of interview questions for Chapter 3. Crucial to this chapter was the context setting and consideration of the incremental development of the Australian regulatory system over time. This chapter considered the circumstances that led to the prioritising of a regulatory response to IBSA in Australia. A discussion of how the regulatory system developed over time in response to various other online harms proved insightful and provided a deeper understanding of the particular manner in which the OESC was established and developed. Particular attention was paid to the operation of the Enhancing Online Safety Act 2015 (the governing legislation of the OESC in place at the time the interviews discussed in Chapter 3 were conducted), but further analysis was carried out following the amendments implemented by the Online Safety Act 2021.

This chapter identified that the criminalisation of IBSA at both state/territory and federal level in Australia has not been a panacea for the challenge of IBSA. Issues around anonymity, jurisdiction, and law enforcement resourcing and training have all hindered the effective combating of IBSA and highlight the need for a supplementary response to the criminal justice process. In particular, a need for a specialist body, with expertise in internet regulation and a mandate in the area of IBSA was identified. The incremental growth in OESC powers and scope from 2015 to 2021 meant that the OESC developed competence and expertise over time demonstrating the importance of targeted reporting mechanisms. This was particularly identified as important in the context of IBSA where the need for an IBA portal equipped with statutory powers to assist in the removal of intimate images was vital. The desk-based assessment of the OESC reporting mechanisms including the Cyberbullying Complaints Scheme, Online Content Scheme and the IBA Portal all provided valuable insight into the practical functioning of the reporting mechanisms of the OESC. In terms of informing the approach taken in conducting interviews, certain issues were identified as requiring deeper exploration through engagement with expert stakeholders. One such issue identified was the need for data concerning time frames from when a complaint is received to when it has been investigated and deemed to be an intimate image or harmful material by the OESC. Prompt response and investigation is vital to ensure that the OESC can take action through the issuing of a removal notice or remedial direction in a timely manner. The publication of this information would provide a clear indication of whether the scheme is operating in an effective manner and could also be used to identify negative trends that may require

corrective action. While the Online Safety Act 2021 requires specific information to be reported in the annual reports, it does not require information on investigation time frames. Chapter 2 also identified that there is a lack of information published about the success of the OESC in assisting in the removal of intimate images permanently – or for an extended period – and it does not appear that the OESC has a system for recording and reporting reoccurring abuse. Chapter 2 identified such a recording and reporting system as necessary in order to better evaluate the effectiveness of the IBA reporting mechanism and to also help identify where additional action may be needed by the OESC. While the OESC can request a service provider located overseas to voluntarily remove harmful content, the OESC had no power to enforce such a request. Circumstances where the offending content is hosted overseas account for the 10-20% of cases where the OESC action fails to result in the removal of content. As a result, Chapter 2 identified the importance of an alternative approach where compelling the direct removal of content is not within the powers of the OESC. Chapter 2 also highlighted the importance of the OESC preventive measures through education, awareness, and collaboration. Based on the review of available publications, Chapter 2 argued that the IBA portal appears to provide a clear, quick, cost effective, and safe mode of complaint and means of redress as an alternative or supplementary measure to criminal prosecution.

The findings from the desk-based analysis supplemented with the literature from key writers in the context of IBSA informed the development of a victim-centred framework identifying the key needs of IBSA victims as:

- constraining distribution of the image
- effective alternatives to constraining the distribution of IBSA images
- adequately trained and resourced authorities
- prompt action
- empowerment
- confidentiality.

Furthermore, the key tools/mechanisms that could be used to address these needs, at least in part, were identified as:

- an independent specialist authority
- individual complaints mechanism
- removal orders

- orders reducing visibility of IBSA material
- statutorily supported codes of practice
- educational campaigns
- civil avenues of redress
- IBSA recognition as a criminal offence.

While the desk-based assessment of the official publications conducted in Chapter 2 provided great insight into the operation of the Australian system, it was clear that interviewing expert stakeholders was necessary in order to delve further into the operation of the OESC in practice and to help answer the questions that were left unanswered by the available published documents. Chapter 3 helps address those gaps by reporting on semi-structured interviews conducted by the author with 14 key stakeholders and by providing an analysis of the key insights obtained.

Chapter 3 identified the importance of engagement with stakeholders by a regulatory body. 13 out of the 14 participants interviews engaged with the OESC on some level. Chapter 3 identified the benefits of such engagement as including greater cooperation, more knowledge exchange, increased awareness raising, and an expanded opportunity to connect with victims through referrals. As a result, Chapter 3 highlighted the importance for the Irish regulatory response to establish clear avenues for stakeholders to engage in order to effectively respond to victim needs. While the OESC has established strong cooperative relationships with the main online platforms and providers, Chapter 3 identified that problems remain with smaller websites which are difficult to locate and refuse to follow the direction of the OESC. As a result, the need of victims to be able to constrain the dissemination of their intimate image is not adequately addressed in every circumstance. Chapter 3 identified weaknesses in the IBA reporting mechanism, particularly that the OESC struggle to assist in the removal of intimate images hosted overseas. Interviews conducted with representatives from the OESC identified the importance of requesting search engines to voluntarily de-index content when they are unsuccessful in assisting removal so to reduce the visibility of the harmful content and therefore address the need of victims for an effective alternative solution to constraining IBSA images. Subsequent to the interviews, the Online Safety Act 2021 further empowered the OESC to issue a link deletion notice so to ensure harmful content would be de-indexed when required. As a result, Chapter 3 highlighted that regulatory attempts in Ireland must consider the possibility that action taken against the provider of the harmful content – particularly where the provider is a smaller platform and/or hosted

overseas – will not always be successful and as a result an alternative course of action must be established in order to mitigate the harm caused and address victim needs. Crucially, Chapter 3 highlighted the importance of an individual complaints mechanism as it provides an alternative or supplementary avenue of complaint and redress for victims in addition to the criminal process or traditional civil approaches. Criminal cases and civil claims can be time consuming, costly, and re-traumatising and therefore sometimes fail to address the need of victims for prompt action. They also carry a risk of bringing greater attention to an issue that a victim may wish to avoid leaving victims need for confidentiality unmet. Furthermore, Chapter 3 identified that the OESC provides an alternative route for victims who are unable to articulate their concerns to platforms or are struggling in their interactions with platforms. As a result, Chapter 3 argued that the Irish regulatory response to IBSA must consider the inclusion of an individual complaints mechanism attached to an adequate system of enforcement ensuring the provision of a fast, free, and less invasive avenue of redress for victims of IBSA thus supporting victim needs for constraining the distribution of IBSA images, effective alternatives to constraining IBSA images, prompt action, empowerment, and confidentiality. Chapter 3 also highlighted that the OESC plays a symbolic role and addresses victim needs for empowerment as it supports victims in regaining some control and provides direct access to a remedy. The mere presence of such a regulatory body has the potential to act as a deterrent to potential perpetrators and can reassure victims that they have a right to pursue justice. As a result, Chapter 3 identified that the awareness-raising and deterrent effect of establishing such a body has the potential to have an impact within the Irish context in addressing victim needs, particularly due to the smaller population and the centralised Governmental structure of the Irish State. While the findings in Chapter 3 broadly support the robust statutory powers of the OESC, the imposing of an enforcement action by the OESC requires a court order which can cause harmful delays to action. As a result, it is argued in Chapter 3 that empowering the OESC to make determinations and directly issue an order or a civil penalty – subject to court appeal – would more effectively address the immediacy and scale of distribution of intimate images in the online sphere thus addressing victim needs more effectively. While the provision of an empowered regulator is essential, Chapter 3 identified the expression of concern by industry that harsh penalties may create a system of uncertainty for social media providers and lead to the removal of legitimate content. These findings underline the importance of due process safeguards and the analysis in Chapter 3 supports the development of an OESC internal review process under the Online Safety Act 2021 to allow for a review of decisions made by the

OESC. Finally, the findings in Chapter 3 indicate that the OESC would benefit from a single entity structure separate to the Australian Communications and Media Authority (ACMA) as this would alleviate existing tensions between members of the OESC and the ACMA and would also lead to better distribution of resources which would allow for the better provision of online safety.

Chapter 4 conducted a comprehensive assessment of the Irish legislative and policy response to IBSA following the enactment of the Harassment, Harmful Communications and Related Offences Act 2020. It was established that while some limited tools/mechanisms that partially responded to the needs of IBSA victims existed in Ireland – particularly following the creation of criminal offences under the Harassment, Harmful Communications and Related Offences Act 2020 – clear gaps in protection remained. In order to provide essential context for the assessment in Chapter 5, Chapter 4 then considered the history and development of the Online Safety and Media Regulation Bill (OSMRB). The regulatory framework outlined in the OSMRB demonstrated the potential to address several of the identified victim needs. Notably, the OSMRB acknowledged the significance of establishing a statutory body with expertise in addressing online harms. An innovative feature introduced by the OSMRB was the 'scheme for notifications by nominated bodies', effectively functioning as a form of systemic 'super-complaints' scheme in conjunction with provision for the future drafting of Online Safety Codes.

Having set out the details of the regulatory framework proposed in the OSMRB in the previous chapter, Chapter 5 engaged in a victim-centred analysis of the OSMRB and of the pertinent amendments to the OSMRB that were included in the OSMRA as enacted. In particular, Chapter 5 used the lessons learned from the desk-based and interview assessment of the functioning of the OESC in practice to assess the potential effect of the Irish OSC as established under the OSMRA 2022. Furthermore, Chapter 5 applied the developed victim-centred framework from previous chapters in order to assess whether the Irish approach effectively addresses victim needs. Recognising the potential of systemic complaint schemes to address victim needs, at least in part, the table representing the victim-centred framework was modified to include 'Systemic complaint scheme' as an additional column representing a mechanism or tool that has the potential to address the needs of victims.

While Chapter 5 acknowledged the potential value of a systemic approach that takes a high-level view of the online environments individuals spend their time in, it was strongly argued that an individual complaints mechanism is necessary if the needs of victims of

IBSA are to be adequately addressed. Chapter 5 identified that with the lack of an individual complaints mechanism in the current regulatory response, the Irish system fails to provide a victim-centred approach which is vital when combating sensitive issues such as IBSA. While the Expert Committee supports the creation of an individual complaints mechanism with a focus on child related issues such as cyberbullying, this thesis recommends that the system should include an IBSA reporting mechanism that allows individuals to directly report cases of IBSA to the OSC. Such a mechanism, attached to robust statutory powers, should also help to empower victims to exercise some control in relation to the harm they have suffered.

The victim-centred framework developed in Chapter 2 highlighted the need of victims to have an alternative solution where constraining the image is impossible. Chapter 5 considered the authority of the OSC to seek a court order to block access to a service which fails to comply with a safety code or content limitation notice. While this mechanism could play an important role in addressing the challenge of rogue services, and would appear to have the potential to respond to the victim need of providing an alternative to constraining the distribution of IBSA images, such actions require an investigation and an application to court. This will likely entail significant delays that may leave an individual victim without a suitable remedy. Furthermore, in the context of an access blocking order, the action works by blocking access to the service completely. While this is perhaps explained by the systemic approach adopted in the Act, such blocking clearly poses a risk to freedom of expression. Due to this and the importance of not denying access to legitimate content, the power is likely to be used sparingly despite its importance in addressing victim needs. Again, this action has the potential to be an important tool in compelling compliance on a systemic level but is likely to leave some victims unprotected.

While the Irish approach affords statutory powers to the OSC to seek a High Court order to compel a designated online service to comply with an Online Safety Code or an order from the High Court to block access to a non-compliant designated online service, Chapter 5 argues that these powers will fall short in addressing victim needs and providing an effective remedy in an online environment whereby a prompt response is essential. Chapter 5 argues that the Irish approach should consider a more empowered regulator with the ability to impose a sanction without a court order subject to appeal in certain circumstances. In order to avoid disproportionate infringements of the right to freedom of expression, different processes could be established depending on the nature

and scope of the order. Furthermore, the establishment of an internal review process for such decisions would provide an important safeguard without the same potential for delay. At all times, of course, such decisions would have to be subject to judicial appeal.

Finally, Chapter 5 argues that the OSC should sit as an independent body separate to Coimisiún na Meán so to avoid disputes regarding funding and the allocation of resources, clashes in authority, and overlapping processes. In order to achieve this, Chapter 5 argues that the Irish legislation should clearly establish the OSC under the OSMRA and separate the OSC as an independent body distinct from Coimisiún na Meán (which deals with a wide array of issues including broadcast regulation). In addition to these practical matters, the separation of the OSC from Coimisiún na Meán to create a highly visible standalone authority with significant expressive and symbolic force would be a gain from the perspective of awareness-raising for all of Irish society and would also better assure victims that their concerns are valid and being taken seriously.

3. Summary of major findings

Whilst this thesis provides detailed key findings specifically relevant to the Australian and Irish regulatory approach to IBSA which have been outlined in the above discussion, there are five major findings which address the ultimate research goal of establishing the best-practice victim-centred regulatory approach for the combating of IBSA. The key findings are listed below as follows:

1. The criminalisation of IBSA alone is insufficient to address the needs of victims of IBSA.
2. The regulation of IBSA is challenging and complex and accordingly the needs of victims of IBSA are best addressed through the use of multiple tools/mechanisms.
    a. The key needs of victims of IBSA were identified as: constraining distribution of the image; effective alternatives to constraining the distribution of IBSA images; adequately trained and resourced authorities; prompt action; empowerment; and confidentiality.
    b. The key tools/mechanisms that could be used to address these needs, at least in part, were identified as: an independent specialist authority; individual complaints mechanism; removal orders; orders reducing visibility of IBSA material; statutorily supported codes of practice; systemic complaint scheme; educational campaigns; civil avenues of

redress; IBSA recognition as a criminal offence. The relationship between these tools/mechanisms are demonstrated in figure 19 below.

3. The application of the victim-centred framework to the Irish approach to IBSA found both evidence of progress and scope for improvement. Of particular note was the finding that while there are benefits to adopting a systemic approach to the regulation of IBSA, an individual complaints mechanism is also necessary to adequately respond to the needs of victims.

Major finding 1: The criminalisation of IBSA alone is insufficient when addressing victims needs.

The applications of the developed victim-centred framework in the Australian and Irish contexts confirmed that the criminalisation of IBSA only partially addresses victim needs. While the Irish Harassment, Harmful Communications and Related Offences Act 2020 and the Australian Criminal Code Act 1995 respond to victim needs for constraining the distribution of IBSA images, empowerment, and confidentiality[2], the response is partial and the criminal law entirely fails to address the other three identified needs. The criminal law fails to provide alternative solutions where removal of the image is unachievable, the lengthy court cases and criminal procedures make the provision of a prompt response unrealistic, and research indicates a clear need for better resourced and trained authorities. As a result, while prior research highlights the limitations of various criminal laws internationally,[3] this research highlights the specific merits and limitations of the criminal law from the perspective of addressing the identified needs of victims.

Major finding 2: The regulation of IBSA is challenging and complex and accordingly the needs of victims of IBSA are best addressed through the use of multiple tools/mechanisms.

This thesis responds to calls for the adoption of a more victim-centred approach to IBSA by developing a victim-centred framework as first set out in Chapter 2.[4] McGlynn and

[2] Confidentiality provided for within the Irish context only.
[3] Nicola Henry, Asher Flynn & Anastasia Powell, 'Policing image-based sexual abuse: stakeholder perspectives' (2018) 19 Police Practice and Research 565; Nicola Henry, Asher Flynn & Anastasia Powell, 'Responding to 'Revenge Pornography': Prevalence, Nature and Impacts' Report to the Criminology Research Advisory Council Grant: CRG 08/15-16 (March 2019); Anastasia Powell & Nicola Henry, 'Policing Technology-Facilitated Sexual Violence Against Adult Victims: Police and Serve Sectors Perspectives' (2016) 28(3) Policing and Society.
[4] See Chapter 2 section 2.9.

others highlight the need for a better understanding of 'the holistic and comprehensive nature of the harms of image-based sexual abuse'[5] in order to 'help to shift law and policy debates towards more comprehensive and effective responses.'[6] As a result, the author developed a victim-centred framework in order to identify the key needs of IBSA victims and the key tools/mechanisms to address those needs.

The key needs of victims of IBSA were identified as: constraining distribution of the image; effective alternatives to constraining the distribution of IBSA images; adequately trained and resourced authorities; prompt action; empowerment; and confidentiality. The key tools/mechanisms that could be used to address these needs, at least in part, were identified as: an independent specialist authority; individual complaints mechanism; removal orders; orders reducing visibility of IBSA material; statutorily supported codes of practice; systemic complaint scheme; educational campaigns; civil avenues of redress; IBSA recognition as a criminal offence.

Below is an abstract table representing the finalised framework and the relationship between the various needs and tools/mechanisms. The plus symbol ('+') indicates the identified potential of a particular mechanism to respond, at least in part, to a particular victim need. While earlier tables were informed by practice in a specific system, this table is populated on the assumption of best practice tools/mechanisms being implemented. For example, a plus symbol is inserted in the cell that intersects with the 'IBSA recognition as a criminal offence' column and the 'Confidentiality' row on the basis that confidentiality can be provided for in the criminal justice system – as it is in the Irish Harassment, Harmful Communications and Related Offences Act 2020 – where legislators bear the needs of victims in mind. Also, a plus symbol is inserted in the cell that intersects with the 'Statutorily supported codes of practice' column and the 'Effective alternatives to constraining IBSA images' row on the basis that an access blocking order and a content limitation notice – as provided for in the Irish context – can be issued resulting from contraventions of Online Safety Codes.

[5] Clare McGlynn, Kelly Johnston, Erika Rackley, Nicola Henry, Nicola Gavey, Anastasia Powell, and Asher Flynn, ''It's Torture for the Soul': The Harms of Image-Based Sexual Abuse' (2020) 30(4) Social and Legal Studies 541-562.
[6] ibid.

Identified tools/mechanisms that address the needs of victims of IBSA

Identified needs of victims of IBSA	*Independent specialist authority*	*Individual complaints mechanism*	*Removal orders*	*Orders reducing visibility of IBSA material*	*Statutorily supported codes of practice*	*Systemic complaint scheme*	*Educational campaigns*	*Civil avenues of redress*	*IBSA recognition as a criminal offence*
Constraining distribution of the image	+	+	+		+	+		+	+
Effective alternatives to constraining IBSA images	+	+		+	+				
Adequately trained and resourced authorities	+						+		
Prompt action	+	+	+	+	+				
Empowerment	+	+					+		+
Confidentiality	+	+							+

Figure 19 Framework table illustrating the relationship between the needs of IBSA victims and the potential tools/mechanisms

This thesis applied the framework originally developed in Chapter 2 in the Australian and Irish contexts in order to better understand how well the different regulatory responses address the needs of victims. It should be noted that the table above includes a column labelled 'systemic complaint scheme' as this research found that the scheme provided for in the Irish OSMRA has the potential to provide additional support for the needs of victims at a systemic level. The continual refining and refracting of the victim-centred framework as occurred throughout the chapters showed that it is only through the existence of a panoply of tools/mechanisms that victim needs are effectively addressed. The removal of a tool/mechanism rendered certain needs unmet. This was particularly evident in the Irish context prior to the enactment of the Online Safety and Media Regulation Act 2022 where the victim need for effective alternatives to constraining IBSA images was entirely unaddressed and the other needs were only partially addressed.

Major finding 3: The application of the victim-centred framework to the Irish approach to IBSA found both evidence of progress and scope for improvement.

The table below represents significant progress made in responding to the needs of victims of IBSA in Ireland in recent years.

Identified tools/mechanisms that address the needs of victims of IBSA

Identified needs of victims of IBSA

	Independent specialist authority	*Individual complaints mechanism*	*Removal orders*	*Orders reducing visibility of IBSA material*	*Statutorily supported codes of practice*	*Systemic complaint scheme*	*Educational campaigns*	*Civil avenues of redress*	*IBSA recognition as a criminal offence*
Constraining distribution of the image	Coimisiún na Meán delegating powers to the Online Safety Commissioner – Online Safety and Media Regulation Act 2022 as initiated, s 6& s 7	Hotline.ie (limited powers and authority)[7]			Online Safety Codes – Online Safety and Media Regulation Act 2022 – s 139K Notice to end contravention - Online Safety and Media Regulation Act 2022, s 139ZZB	Systemic complaint scheme – Online Safety and Media Regulation Act 2022, s 139ZC		Civil remedies, including damages and injunctive relief available	Harassment, Harmful Communications and Related Offences Act 2020, s 2 & s 3
Effective alternatives to constraining IBSA images	Coimisiún na Meán delegating powers to the Online Safety Commissioner – Online Safety and Media Regulation Act2022, s 6 & s 7				Access blocking order & Content limitation notice- Online Safety and Media Regulation Act 2022, s 139ZZC & s139ZZD (resulting from contraventions of online safety codes)				
Adequately trained and resourced authorities	Coimisiún na Meán delegating powers to the Online Safety Commissioner – Online Safety and Media Regulation Act 2022, s 6 & s 7	Hotline.ie (limited powers and authority)[8]					Action Plan for Online Safety 2018/2019 – Action 1-5, 8, 9		
Prompt action	Coimisiún na Meán delegating powers to the Online Safety Commissioner – Online Safety and Media Regulation Act 2022, s 6 & s 7	Hotline.ie (limited powers and authority)[9]			Notice to end contravention - Online Safety and Media Regulation Act 2022, s 139ZZB				
Empowerment	Coimisiún na Meán delegating powers to the Online Safety Commissioner – Online Safety and Media	Hotline.ie (limited powers and authority)[10]					Action Plan for Online Safety 2018/2019 – Action 1-5, 8, 9		Harassment, Harmful Communications and Related Offences Act 2020, s 2 & s 3

[7] Hotline.ie is a non-profit national reporting mechanism whereby members of the public can report concerns in respect of illegal content online. It has the power to inform service providers of the existence of suspected IBSA on their platform who may voluntarily remove the material as a result. They also refer suspected IBSA to An Garda Síochána.

[8] ibid.

[9] ibid.

[10] ibid.

	Regulation Act 2022, s 6 & s 7								
Confidentiality									Harassment, Harmful Communications and Related Offences Act 2020, s 5

Figure 18 Framework table of key needs and identified tools/mechanisms applied in the Irish context incorporating the Online Safety and Media Regulation Act

As already noted, the criminalisation of IBSA in the Harassment, Harmful Communications and Related Offences Act 2020 was a significant step forward and the OSMRA has the potential to create a safer online environment for all, including for victims of IBSA. It should be noted, however, that while Ireland addresses in some way each of the identified needs of victims of IBSA, there are serious limitations to several of the responses. While Hotline.ie provides a limited form of response to several of the identified victim needs, the limited nature of its functions, its lack of statutory powers, and the voluntary nature of any compliance with removal requests made by the body mean that it cannot be considered directly comparable to the tools established in Australia.

Another example concerns the importance of an independent specialist body. While the OSMRA identified a role for the Online Safety Commissioner, the Commissioner must operate within the structure of Coimisiún na Meán and questions about its ability to obtain sufficient resourcing and staff have already been raised.[11] Its operation within the broader Commission also hinders its recognition as a significant national body with a high public profile. The role the OSC will play will only fully begun to be understood once Online Safety Codes begin to be published.

An important innovation of the OSMRB was the 'scheme for notifications by nominated bodies' which was designed to function as a type of 'super-complaints' system. While a systemic complaints scheme may not address the same needs that are addressed by an individual complaints mechanism, the potential of such schemes to address victim needs at a high level, at least in part, is recognised.

A significant issue with the OSMRA is the failure to provide for an individual complaints scheme for victims of IBSA. While such a scheme is possible under the Act, there is no

[11] Michael Brennan, 'Online Safety Commissioner May Need up to 5,000 Staff and €407m Budget' *Business Post* (24 September 2022).

intention of introducing such a system at least in the coming years. While a systemic approach is valuable, an individual complaints mechanism is necessary to adequately empower victims of IBSA. While Hotline.ie allows individuals to report cases of IBSA, it does not have any statutory power to assist in the removal of IBSA images. Hotline.ie can only request the removal of a reported image however has no power to enforce its request if such a request is not followed. As a result, Hotline.ie does not provide the necessary support required by victims compared to the IBA portal in the Australian context. As evident in the Australian context, an individual complaints mechanism addresses victim needs for image removal, alternative solutions, prompt action, empowerment, and confidentiality. However, the lack of such a system in the Irish context leaves these needs only partially addressed through the other identified tools/mechanisms. As a result, this thesis greatly supports the inclusion of an individual complaints mechanism for victims of IBSA in order to adequately address victim needs. While the Irish response provides for notices to end contraventions with online safety codes and access blocking orders again in the context of online safety code violations, the Irish system fails to provide for removal orders and orders reducing the visibility of images which can be issued directly to end users. While the removal of IBSA images can be addressed at the systemic level it also needs to be addressed at the end-user level.

4. Reflections for Ireland

Any regime established to govern online safety will need continuous attention as the challenges and opportunities in this space change at a rapid pace. Not only is the underlying technology and its implementation always evolving, but so is the manner in which individuals engage with the technology and connect with each other virtually. Legislators and policy-makers must remain responsive to these changes and ensure that the needs of victims are being adequately addressed. Due to the nascent nature of the Irish regulatory system for online safety, there is scope for continued research on the functioning of the approach adopted in the OSMRA, particularly as Online Safety Codes are drafted and online platforms are designated as relevant services. Furthermore, the form, structure, and scope of any possible individual complaints mechanism has yet to be decided. As a result, ongoing research into the functioning of the Irish system in practice will be essential in ensuring that the challenge of IBSA is being tackled effectively.

In order to provide adequate transparency, the Irish OSC should need to report on the number of complaints it receives, the length of time taken to conduct an investigation, the number of notices issued, the number of alternative actions taken where removal is not possible, and the length of time taken by platforms to remove the reported content following a notice. Similar to the desk-based research conducted on the OESC annual reports, an assessment of this data over a period of time will allow for a clear understanding of whether the implemented body is effective in practice or whether amendments to the OSMRA are necessary (as seen in Chapter 2 with the many amendments made over time in the Australian context). While this thesis argues strongly for the adoption of an individual complaints mechanism and the Act was amended at Committee stage to allow for the potential establishment of an individual complaints scheme, such a scheme will take time to develop and it has been suggested that if such a scheme is implemented in the coming years, the focus will be on harms particular to children. While the systemic complaint scheme has the potential to address high-level issues and to encourage compliance with Online Safety Codes, there is a risk that a systemic complaint scheme's reliance on 'notifications by nominated bodies' might be perceived as gatekeeping and victims may feel locked out from this new authority as a result.

While the implementation of a new regulatory system to address the harms of IBSA is endorsed by this research, there is a need for additional cultural change and greater awareness that the recording and/or distribution of intimate images is entirely unacceptable. The law plays a vital – but ultimately limited – role in bringing about that change. As a result, the OSMRA will have to be supplemented by national educational campaigns with a focus on informing individuals on the harms of IBSA and the legal mechanisms in place designed to address those harms, including through the criminal justice and online safety regulatory systems. While Minister Martin has spoken about how the Online Safety Commissioner will 'have a role in producing, coordinating and supporting online safety educational initiatives and research', this is not specifically provided for in the Act.[12] It is not only important that the OSC carries out this educative

[12] Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media, 'Minister Martin Launches Comprehensive Online Safety Research on Internet Use by Children and Adults' (Press Release, 15 November 2021) < gov.ie - Minister Martin launches comprehensive online safety research on internet use by children and adults (www.gov.ie)> accessed 23 May 2023. There is some general reference to promoting educational initiatives as part of the broad remit of the Commission, referring to media literacy in particular, but there is no specific reference to a special role for the OSC, or even the Commission, in relation to Online Safety education and training. Online Safety and Media Regulation Act, s.7 (3)(g).

function, but also that the Commissioner is adequately resourced to fulfil the function at the level and scale necessary.

5. Reflections for other jurisdictions

The examination of the Australian and Irish responses to online safety show that general lessons can be learned and applied in other jurisdictions seeking to implement a regulatory system and authority designed to combat online harm including IBSA. While early responses to IBSA in Australia and Ireland oriented towards self-regulation through voluntary content removal by online platforms, the past few years have seen a decisive shift in favour of statutory regulation. In particular, the Irish and Australian approaches have highlighted that while traditional civil and criminal approaches are important, an alternative approach is also necessary through the implementation of a regulatory authority that encourages reporting, has enforcement powers, educates users, and empowers victims. The affording of statutory enforcement powers is essential to ensure that a regulatory body is adequately equipped to make a real impact. Without the power to issue a notice for removal or take an enforcement action, the effectiveness of any regulatory authority will be undermined. The application of the victim-centred framework in this thesis revealed the merit of an individual complaints scheme. Without such a scheme, a barrier may be created for victims to report issues or seek justice. The importance of alternative actions where the preferred goal of content removal is impossible is also clear in order to address the challenges posed by jurisdiction and anonymity in the online environment. Notwithstanding the importance of an individual complaints scheme, the needs of victims can also be partially addressed by the use of a systemic approach designed to ensure that the environments in which online interactions occur do not facilitate the perpetration of IBSA.

Jurisdictions seeking to regulate in this space should consider a comprehensive approach where consistency in processes leads to greater clarity, foreseeability, transparency, and efficiency whilst still leaving flexibility for special rules or measures in the context of specific online harm issues. Furthermore, while national action is important, there is also merit in adopting EU or international approaches due to the borderless nature of the internet and the many issues that occur when trying to remove IBSA hosted outside of your own state. The adoption of EU and international approaches can lead to consistency across jurisdictions which may result in faster more efficient removal of IBSA material.

Indeed, the Digital Services Act is likely to become increasingly influential as its provisions begin to come into effect.

6. Broader applicability of the developed victim-centred framework

This thesis developed a victim-centred framework in order to assess the effectiveness of legislative responses to IBSA. The importance of identifying the needs of victims as a key factor in the development of such a framework in order to assess to what extent a legislative response is effective was highlighted. Having been initially informed by desk-based research of the Australian system and by the academic literature, the framework was refined through consideration of stakeholder interviews and the Irish response to IBSA. It is suggested that the framework could be used to assess the laws and policies of other jurisdictions in order to consider whether those systems adequately respond to the needs of victims of IBSA. Moreover, due to the commonalities between the harms and challenges of IBSA and other forms of online harm, the framework could also serve as a useful starting point for considering whether systems designed to address other types of harms – such as cyberbullying – are sufficiently responsive to the needs of victims.

7. Concluding comment

Overall, this thesis has highlighted that the regulation of IBSA is a complex issue which requires additional attention in the Irish context from a victim-centred perspective. While progress has been made through the enactment of the Harassment, Harmful Communications and Related Offences Act 2020 and the OSMRA, significant improvements are necessary in order to better address the challenge of IBSA and more effectively respond to the needs of victims. Due to the constantly evolving online environment, the uncertain content of the forthcoming Online Safety codes, and the unresolved status of an individual complaints scheme, it is clear that ongoing research into the operation and effectiveness of the system from a victim-centred perspective will continue to be necessary. As a result, the framework developed in this thesis has the potential to assess future developments in the law.

Bibliography

Journal Articles

Akdeniz Y, 'Governance of Pornography and Child Pornography on the Global Internet: A multi layered approach, in law and in the internet' (1997) Regulating Cyberspace 223

Bachrach C, 'The case for a safe harbor provision of CDA 230 that allows for injunctive relief for victims of fake profiles' (2020) 72 Federal Communications Law Journal 147

Baez B, 'Confidentiality in qualitative research: Reflections on secrets, power and agency' (2002) 1(2) Qualitative Research 35

Barcan R, 'In the raw: 'Home-made' porn and reality genres' (2002) 3(1) Journal of Mundane Behaviour

Bates S, 'Revenge porn and mental health: A qualitative analysis of the mental health effects of revenge porn on female survivors' (2016) 12(1) Feminist Criminology 22

Berners-Lee T, Cailliau R, Groff J, Pollermann B, 'World Wide Web: The Information Universe' (1992) 2 Electronic Netwroking 52

Bhat I, *'Comparative Method of Legal Research Nature, Process, and Potentiality' Ideas and Methods of Legal Research* (Oxford University Press 2019)

Bond E, & Tyrrell K, 'Understanding Revenge Pornography: A National Survey of Police Officers and Staff in England and Wales' (2021) 36 Journal of Interpersonal Violence 2166

Bothamley S, & Tully R.J, 'Understanding revenge pornography: public perceptions of revenge pornography and victim blaming' (2017) 10(1) Journal of Aggression, Conflict and Peace Research

Boyd D.M, & Ellison N.B, 'Social Network Sites: Definition, History, and Scholarship' (2008) 13 Journal of Computer-Mediated Communication 210

Branch K, Hilinski-Rosick C. M, Johnson E, & Solano G. 'Revenge porn victimization of college students in the United States: An exploratory analysis' (2017) 11(1) International Journal of Cyber Criminology 128

Brunner L, 'The Liability of an Online Intermediary for Third Party Content The Watchdog Becomes the Monitor: Intermediary Liability after Delfi v Estonia' (2016) 16 Human Rights Law Review 163

Calvert C, & Brown J, 'Video Voyeurism, Privacy, and the Internet: Exposing Peeping Toms in Cyberspce' (2000) 18 Cardozo Arts & Entertainment Law Journal 469

Citron D, & Franks A, 'Criminalizing revenge porn' (2014) 49 Wake Forest Law Review 345

Citron D, 'Sexual Privacy' (2019) 128(7) The Yale Law Journal 1870

Curran V, ‘Cultural Immersion, Difference and Categories in US Comparative Law’ (1998) 46(1), American Journal of Comparative Law 43

Daly T, ‘Strengthening Irish Democracy: A Proposal to Restore Free Speech to Article 40.6.1°(I) of the Constitution’ (2009) 31(1) Dublin University Law Journal 228

D’Amico E, & Steinberger L, 'Fighting for Online Privacy with Digital Weaponry: Combating Revenge Pornography' (2015) 26 NYSBA Entertainment, Arts and Sports Law Journal 24

Daniels M, ‘Chapters 859 & 863: Model Revenge Porn Legislation or Merely a Work in Progress?’ (2014) 46 McGeorge Law Review 297

Dant T, & Gilloch G, ‘Pictures of the Past: Benjamin and Barthes on Photography and History’ (2002) 5(1) European Journal of Cultural Studies 5

Davenport D, ‘Anonymity on the Internet: Why the Price May Be Too High’ (2002) 45 Communications of the ACM 33

Dawkins J, ‘A Dish Served Cold: The Case for Criminalizing Revenge Pornography’ (2015) 45 Cumberland Law Review 395

DeKeseredy W, & Schwartz M, ‘Thinking Sociologically About Image-Based Sexual Abuse: The Contribution of Male Peer Support Theory’ (2016) Sexualization, Media, & Society

Dhar V, & Chang E.A, ‘Does Chatter Matter? The Impact of User-Generated Content on Music Sales’ (2009) 23(4) Journal of Interactive Marketing 300

Dickson A, ‘Revenge Porn: A Victim Focused Response’ (2016) 2 UniSA Student Law Review 42

Dolliver D, ‘Evaluating Drug Trafficking on the Tor Network: Silk Road 2, the Sequel’ (2015) 26(11) International Journal of Drug Policy 1113

Etikan I, ‘Comparison of convivence sampling and purposive sampling’ (2016) 5(1) American Journal of Theoretical and Applied Statistics

Farries E, ‘Feminist legal geographies of intimate-image sexual abuse: Using copyright logic to combat the unauthorized distribution of celebrity intimate images in cyberspaces’ (2019) 51 EPA: Economy and Space 1145

Fido D, Rao J, & Harper C.A, ‘Celebrity status, sex, and variation in psychopathy predicts judgements of and proclivity to generate and distribute deepfake pornography’ (2022) 129 Computers in Human Behaviour

Flanagan B, & Ahern S, ‘Judicial Decision-Making and Transnational Law: A Survey of Common Law Supreme Court Judges’ (2011) 60(1) International & Comparative Law Quarterly 1

Flynn A, & Henry N, 'Image-Based Sexual Abuse: An Australian Reflection' (2021) 31(4) Women & Criminal Justice 313

Flynn A, Powell A, Scott A, & Cama E, 'Deepfakes and Digitally Altered Imagery Abuse: A Cross-Country Exploration of an Emerging form of Image-Based Sexual Abuse' (2021) British Journal of Criminology

Franks M, 'Drafting an Effective 'Revenge Porn' Law: A Guide for Legislators' (2016) 3

Ghafel R, 'From enabling to levelling: the need to change the policy rationale of the intermediary liability regime' (2016) 25 Information & Communications Technology Law 129

Gilden M, 'Jurisdiction and the Internet: The 'Real World' meets cyberspace' (2000) 7(1) ILSA Journal of International & Comparative Law 149

Gillespie A.A, '"Up-Skirts" and "Down-Blouses:" Voyeurism and the Law' (2008) Criminology Law Review 370

Gillespie T, et al, 'Expanding the debate about content moderation: Scholarly research agendas for the coming policy debates' (2020) 9(4) Internet Policy Review

Gillooly M & Nii Wallace-Bruce N, 'Civil Penalties in Australian Legislation' (1994) 13 University of Tasmania Law Review 269

Goldnick L, 'Coddling the Internet: How the CDA Exacerbates the Proliferation of Revenge Porn and Prevents a Meaningful Remedy for its Victims' (2015) 21 Cardozo Journal or Law & Gender 583

Goldsmith J.L, 'Against Cyberanarchy' (1998) 65 University of Chicago Law Review 1199

Goldsmith J.L, 'The Internet and the Abiding Significance of Territorial Sovereignty' (1998)5 Indiana Journal Global Legal Studies 475

Gorwa R, Binns R, & Katzenbach C, 'Algorithmic content moderation: Technical and political challenges in the automation of platform governance' (2020) 7(1) Big Data & Society

Gorwa R, 'What is platform governance?' (2018) 22 Information, Communication & Society 854

Griffith V.N, 'Smartphones, Nude Snaps, and Legal Loopholes: Why Pennsylvania Needs to Amend its Revenge Porn Statute' (2016) 16 Journal of Technology Law and Policy 135

Harika A, 'Banning Revenge Pornography: Florida' (2014) 39 Nova Law Review 65

Harris D, 'Deepfakes: False pornography is here and the law cannot protect you' (2018) 17 Duke Law and Tecchnology Review 99

Henry N, & Flynn A, ‘Image-based sexual abuse: Online distribution channels and illicit communities of support’ (2019) 25 Violence Against Women 1932

Henry N, Flynn A, & Powell A, ‘Policing image-based sexual abuse: stakeholder perspectives’ (2018) 19(6) Police Practice and Research 565

Henry N, & Powell A, ‘Beyond the “sext”: Technology-facilitated sexual violence and harassment against adult women’ (2015) 48(1) Australian & New Zealand Journal of Criminology 104

Hermes J, ‘Section 230 as Gatekeeper: When Is an Intermediary Liability Case Against a Digital Platform Ripe for Early Dismissal?’ (2017) 43 American Bar Association 34

Hilbert M, ‘The bad news is that the digital access divide is here to stay: Domestically installed bandwidths among 172 countries for 1986–2014’ (2016) Telecommunications Policy

Hill R, ‘Cyber-misogyny: should ‘revenge porn’ be regulated in Scotland, and if so, how?’ (2015) 12(2) SCRIPTed

Holm E, ‘The Darknet: A New Passageway to Identity Theft’ (2017) 6(1) International Journal of Information Security and Cybercrime 41

Homchick N, ‘Reaching Through the "Ghost Doxer:" An Argument for Imposing Secondary Liability on Online Intermediaries’ (2019) 76 Washington & Lee Law Review 1307

Hughes T, ‘Regulation of the Net’ (1997) 71 The IT Age: law and information technology

Humbach J, ‘The Constitution and Revenge Porn’ (2014) 35 Pace Law Review 215

Jacobs A, ‘Fighting back against revenge pornography: a legislative solution’ (2016) 12(1) Northwerstern Journal of Law and Social Policy

Johnston D.R, & Post D.G, ‘Law and Borders – The rise of Law in Cyberspace’ (1996) 48 Stanford Law Review 1367

Kaiafa-Gbandi M, ‘Criminalizing Attacks against Information Systems in the EU: The Anticipated Impact of the European Legal Instruments on the Greek Legal Order’ (2012) 20(1) European Journal of Crime, Criminal Law, and Criminal Justice 59

Kallen D, ‘Mark Zuckerberg, Joe Manchin, and ISIS: What Facebook's International Terrorism Lawsuits Can Teach Us About the Future of Section 230 Reform’ (2021) 100 Texas Law Review

Kerr O.S, ‘The Problem of Perspective in Internet Law’ (2003) 91 Georgetown Law Journal 357

Kuczerawy A,’ Intermediary liability & freedom of expression: Recent developments in the EU notice & action initiative’ (2015) 31 Computer Law & Security Review 46

Lake J, '"Overexposed": Legal Responses to the Unauthorised Publication of Private Photos' (2016) 3 Australian Media, Technology and Communications Law Bulletin 8

Larkin P.J, 'Revenge Porn, State Law, Free Speech' (2014) 48 Loyola of Los Angeles Law Review 24

Lauckner C, Truszczynski N, Lambert D, Kottamasu V, Meherally S, Schipani-McLaughlin A, Taylor E, & Hansen N, 'Catfishing, cyberbullying, and coercion: An exploration of the risks associated with dating app use among rural sexual minority males' (2019) 23(3) Journal of Gay & Lesbian Mental Health 289

Legrand P, 'Comparative Legal Studies and the Matter of Authenticity', (2006) 1(2), Journal of Comparative Law 365

Lemley M, 'Place and Cyberspace' (2003) 91 California Law Review 521

Lerner M.J, & Miller D.T, 'Just world research and the attribution process: looking back and ahead' (1978) 85 Psychological Bulletin 1030

Levendowski A, 'Using Copyright to Combat Revenge Porn' (2014) N.Y.U Journal of Intellectual Property and Entertainment Law 422

Linkous T, 'It's Time for Revenge Porn to Get a Taste of Its Own Medicine: An Argument for the Federal Criminalization of Revenge Porn' (2014) 20 Richmond Journal of Law and Technology 14

Maddocks S, 'From Non-consensual Pornography to Image-based Sexual Abuse: Charting the Course of a Problem with Many Names' (2018) 33 Australian Feminist Studies 345

Magaldi J.A, Sales J.S, & Paul J, 'Revenge Porn: The Name Doesn't Do Nonconsensual Pornography Justice and the Remedies Don't Offer the Victims Enough Justice' (2020) 98 Oregon Law Review 197

Mann K, 'Punitive Civil Sanctions: The Middle ground Between Criminal and Civil Law' (1992) 101(5) Yale Law Journal 1795

Martines C, 'An argument for Sates to Out Law Revenge Porn and for Congress to Amend 4
U.S.C and 230: How our Current Laws Do Little to Protect Victims' (2014) 14 Pittsburgh Journal of Law and Policy 235

Mascheroni G, Vincent J, & Jinenez E. '"Girls are addicted to likes so they post semi-naked selfies": Peer mediation, normativity and the construction of identity online' (2015) 9(1) Cyberpsychology: Journal of Psychosocial Research on Cyberspace

Matsui S, 'The criminalization of revenge porn in Japan' (2015) 24(2) Washington International Law Journal 289

McCartan K.F, & McAlister R, 'Mobile phone technology and sexual abuse' (2012) 21(3) Information & Communications Technology Law 257

McGlynn C, & Rackley E, ‘Image-Based Sexual Abuse: More than just ‘Revenge Porn’’ (2016) Research Spotlight

McGlynn C, & Rackley E, 'Image-Based Sexual Abuse' (2017) 37 Oxford Journal of Legal Studies 534

McGlynn C, & Rackley E, ‘More than ‘Revenge Porn’: Image-Based Sexual Abuse and the Reform of Irish Law’ (2017) 14 Irish Probation Journal 38

McGlynn C, Rackley E, & Houghton R, ‘Beyond “revenge porn”: The continuum of image-based sexual abuse’ (2017) 25(1) Feminist Legal Studies 256

McGlynn C, Rackley E, Johnson, Henry N, Gavey N, Flynn A, Powell A, & Scott A, ‘It’s Torture for the Soul”: the harms of image-based sexual abuse’ (2020) 30(4) Social and Legal Studies 541

McKenna K, & Bargh J, ‘Plan 9 from Cyberspace: The Implications of the Internet for Personality and Social Psychology’ (2000) 4 Personality and Social Psychology Review 60

Miller S, ‘Perspective Jurisdiction over internet activity: The Need to Define and Establish the Boundaries of Cyberlibert’ (2003) 10 Indiana Journal of Global Legal Studies 227

Milosevic T, & Vladisavljevic M, ‘Norwegian children’s perceptions of effectiveness of social media companies’ cyberbullying policies: an exploratory study’ (2020) 14(1) Journal of Children and Media 74

Mirea M, Wang V, & Jung J, ‘The not so dark side of the darknet: a qualitative study’ (2019) 32(2) Security Journal 102

Montagnani M.L, Safe harbours in deep waters: a new emerging liability regime for Internet intermediaries in the Digital Single Market (2018) 26 International Journal of Law and IT 294

Moore D, & Rid T, ‘Cryptopolitik and the Darknet’ (2016) 58 (1) Survival Global Politics and Strategy 7

Muñiz A.M, Jensen H, & Vigilante S, ‘Marketing and Consumer-Created Communications’ (2007) 36(3) Journal of Advertising 35

Murray A, ‘Nodes and Gravity in Virtual Space’ (2011) 5 Legisprudence 195

Nolan, M. P, ‘Learning to circumvent the limitations of the written-self: The rhetorical benefits of poetic fragmentation and internet ‘catfishing’’ (2015) 1(1) Persona Studies 53

O’Dell E, ‘Compensation for Breach of the General Data Protection Regulation’ (2017) 40(1) Dublin University Law Journal 97

Omer C, ‘Intermediary Liability for Harmful Speech: Lessons from Abroad’ (2014) 28(1) Harvard Journal of Law & Technology 289

Owen G, & Savage N, ‘Empirical Analysis of Tor Hidden Services’ (2016) 10(3) IET Information Security 113

Phillipson G, ‘Max Mosley goes to Strasbourg: Article 8, Claimant Notification and Interim Injunctions’ (2009) 1 Journal of Media Law 73

Pitcher J, ‘The State of the States: The Continuing Struggle to Criminalize Revenge Porn’ (2016) 2015 Brigham Young University Law Review 1435

Post D, ‘Against ‘Against Cyberanarchy’ (2002)17 Berkeley Technology Law Journal 1365

Post D, 'Governing Cyberspace: The Law' (2008) 24 Santa Clara Computer and High Technology Law Review 883

Poltash N, ‘Snapchat and Sexting: A snapshot of baring your Bare essentials’ (2014) 19(4) Richmond Journal of Law and Technology 1

Powell A, & Henry N, ‘Blurred Lines? Resonding to ‘Sexting’ and Gender-based Violence amoung Young People’ (2014) 39(2) Children Australia 119

Powell A, & Henry N, ‘Policing technology-facilitated sexual violence against adult victims: Police and serve sectors perspectives’ (2016) 28(3) Policing and Society

Powell A & Henry N, ‘Sexual Violence in the Digital Age: The Scope and Limits of Criminal Law’ (2016) 25(4) Social & Legal Studies 397

Powell A, & Henry N, ‘Technology-facilitated sexual violence victimization: Results from an online survey of Australian adults’ (2019) 17 Journal of Interpersonal Violence 34

Priebe G, & Svedin C. G, ‘Online or off-line victimization and psychological wellbeing: A comparison of sexual-minority and heterosexual youth’ (2012) 21(10) European Child & Adolescent Psychiatry 569

Purtova N, ‘Private Law Solutions in European Data Protection: Relationship to Privacy, and Wavier of Data Protection Rights’ (2010) 28(2) Netherlands Quarterly of Human Rights 179

Reed L, Tolman R, & Ward M, ‘Snooping and sexting: Digital media as a context for dating aggression and abuse among college students’ (2016) 22(13) Violence Against Women 1556

Resnik D, ‘What is Ethics in Research & Why is it Important?’ (2011) National Institute of Environmental Health Studies

Ringrose J, & Renold E, ‘Slut-shaming, girl power and ‘sexualisation’: Thinking through the politics of the international SlutWalks with teen girls’ (2012) 24(3) Gender and Education 333

Ryan E, ‘Sexting: How the State can prevent a moment of indiscretion from leading to a lifetime of unintended consequences for minors and young adults’ (2010) 96 Iowa Law Review 357

Russ M, ‘Problematically Proactive: a Summary of Recent Legal Developments In the Field of Internet Intermediary Liability’ (2018) 69 Northern Ireland Legal Quarterly 563

Satti C, ‘A Call to (Cyber) Arms: Applicable Statutes and Suggested Courses of Action for the Celebrity iCloud Hacking Scandal’ (2016) 34 Quinnipiac Law Review 561

Sechenova M, ‘Fahrenheit 451: burning through the great firewall of China’ (2016) 3 The Indonesian Journal of International & Comparative Law: Socio-Political Perspectives

Senft T, & Baym N, ‘What Does the Selfie Say? Investigating a Global Phenomenon’ (2015) 9 International Journal of Communication1588

Silva A.N, & Reed C, ‘You can’t always get what you want: Relative anonymity in cyberspace’ (2015) 12(1) Scripted

Scheller S.H, ‘A picture is worth a thousand words: The Legal Implications for Revenge Pornography’ (2015) 93 North Carolina Law Review 551

Schwartz P.M, ‘Privacy and Democracy in Cyberspace’ (1999) 52 Vanderbilt Law Review 1607

Smith A, Fischer E, & Yongjian C, ‘How Does Brand-related User-generated Content Differ across YouTube, Facebook, and Twitter?’ (2012) 26 Journal of Interactive Marketing 102

Solove D, ‘The PII problem: Privacy and a New Concept of Personally Identifiable Information’ (2011) 86 New York University Law Review 1814

Sorensen J.M, ‘Forgive and Regret: Analysis and Proposed Changes to Connecticut's Revenge Porn Statute’ (2017) 35 Quinnipiac Law Review 559

Spivak R, ‘"Deepfakes": The newest way to commit one of the oldest crimes’ (2019) 3 Georgetown Law Technology Review 339

Srivastava A, & Thomson S.B, ‘Framework Analysis: A Qualitative Methodology for Applied Policy Research’ (2009) 4(2) JOAAG 72

Stroud S.R, ‘The dark side of the online self: A pragmatic critique of the growing plague of revenge porn’ (2014) 29 Journal of Mass Media Ethics 168

Suler J,’ The Online Disinhibition Effect’ (2004) 7 Cyber psychology & behaviour 321

Suzor N, Seignior B, & Singleton J, ‘Non-consensual porn and the responsibilities of online intermediaries’ (2017) 40(3) Melbourne University Law Review 1057

Svantesson D, ‘Sexting and the law: How Australia regulates electronic communication of non-professional sexual content’ (2010) 22(2) Bond Law Review 41

Synodinou T.E, ‘Geoblocking in EU Copyright Law: Challenges and Perspectives’ (2020) 69 GRUR International, Journal of European and International IP law 136

Tbakhi A, & Amr S, ‘Ibn Al-Haytham: Father of Modern Optics’ (2007) 27(6) Ann Saudi Med 464

Thompson C, & Wood M.A, ‘A media archaeology of the creepshot’ (2018) 18(4) Feminist Media Studies 560

Tobin G, & Begley C, ‘Methodological rigour within qualitative framework’ (2004) 48(4) Journal of Advanced Nursing 388

Toma C. L., Hancock J. T, & Ellison N. B, ‘Separating fact from fiction: An examination of deceptive self-presentation in online dating profiles’ (2008) 34(8) Personality and Social Psychology Bulletin 1023

Vigdor J, Ladd H, & Martinez E, ‘Scaling the digital divide: Home computer technology and student achievement’ (2014) 52 Economic Inquiry 1103

Waldman A.E, ‘A Breach of Trust: Fighting Nonconsensual Pornography’ (2017) 102 Iowa Law Review 709

Walker S, Sanci L & Temple-Smith M, ‘Sexting: Young women’s and men’s views on its nature and origins’ (2013) 52 Journal of Adolescent Health 697

Walley P, ‘In Memory Amore: Revenge, Sex and Cyberspace’ (2015) 20(2) The Bar Review 33

Warren S, & Brandeis L, ‘The Right to Privacy’ (1890) 4(5) Harvard Law Review 193

Won Kim J, & Chock T.M, ‘Personality traits and psychological motivation predicting selfie posting behaviours on social networking sites’ (2017) 34 Telematics and Informatics 560

Wood M, Barter C, Stanley N, Aghtaie N, & Larkins C, ‘Images across Europe: The sending and receiving of sexual images and associations with interpersonal violence in young people's relationships’ (2015) 59 Children and Youth Services Review 149

Yar M, & Drew J, ’Image-Based Abuse, Non-Consensual Pornography, Revenge Porn: A Study of Criminalization and Crime Prevention in Australia and England & Wales’ (2019) 13 International Journal of Cyber Criminology 578

Zimmerman D.L, ‘Requiem for a Heavy weight: A Farewell to Warren and Brandeis's Privacy Tort’ (1983) 68 Cornell Law Review 291

Zittrain J, What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication, (2000) 52 Standford Law Review1201

Books

Barendt E, *Freedom of Speech* (2nd edn, Oxford University Press 2006)

Berger J, *Ways of Seeing* (London: Viking Books 1972)

Bernard H.R, *Research methods in anthropology: Qualitative and quantitative approaches* (3rd edn, Walnut Creek, CA: Alta Mira Press 2002)
Boyatzis R, Transforming Qualitative Information: Thematic Analysis and Code Development (Sage: USA, 1998)

Citron D, *Hate Crimes in Cyberspace* (1st edn, Harvard University Press 2014)

Cohen J, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (New Haven, CT: Yale University Press 2012)

Crane B, *Using Web 2.0 and Social Networking Tools in the K-12 Classroom* (American Library Association 2012)

Cresswell J.W, & Plano Clark V.L, *Designing and Conducting mixed method research* (2nd edn, Thousand Oaks, CA: Sage 2011)

Cresswell J.W, *Research Design: Qualitative, Quantitative, and Mixed Research Methods* (Sage, 2013)

Fenwick H, & Phillipson G, *Media Freedom under the Human Rights Act* (Oxford University Press, 2006)

Gillespie T, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (1st edn, New Haven CT: Yale University Press 2018)

Goldstein A, *The Psychology of Group Aggression* (John Wiley and Sons 2002)

Gooch G, & Williams M, *A Dictionary of Law Enforcement* (2nd edn, Oxford University Press 2015)

Gottschalk P, *Policing Cyber Crime* (1st edn, Bookboon 2010)

Hall M, & Hearn J, *Revenge Pornography Gender, Sexualities and Motivations* (Routledge: New York 2018)

Henry N, McGlynn C, Flynn A, Johnson K, Powell A, & Scott A, '*Image-Based Sexual Abuse: A Study on the Causes and Consequences of Non-Consensual Nude or Sexual Imagery*' (1st edn, Routledge 2020)

Hogg M.A, & Vaughan G.M, *Social Psychology* (4th edn, Pearson Education Limited Essex 2015)

Ivester Matt, *lol . . .OMG! What Every Student Needs to Know about Online Reputation Management, Digital Citizenship and Cyberbullying* (Reno, NV: Serra Knight, CreateSpace Independent Publishing Platform 2011)

Joinson A, *Understanding the Psychology of Internet Behaviour: Virtual Worlds, Real Lives* (Palgrave Macmillan 2003)

Kennedy R & Murphy M.H, *Information and Communications Technology Law in Ireland* (1st edn Clarus Press 2017)

Lessig L, *The Future of Ideas: The fate of the Commons in a Connected World* (1st edn, Random House 2001)

Lessig L, *Code Version 2.0* (2nd edn, Basic Books 2006)

Marx G, 'What's in a Name? Some Reflections on the Sociology of Anonymity' (1999) 15 The Information Society 99

Mullen B, 'Operationalizing the Effect of the Group on the Individual: A Self-Attention Perspective' (1983) 19 Experimental Social Psychology Journal 295

Murray A, *Information Technology Law: The law and Society* (2nd edn., Oxford University Press 2010)

Murray A, *Information Technology Law and Society* (3rd edn, New York: Oxford University Press 2016)

Newhall B, *The History of Photography: From 1839 to the Present* (New York, The Museum of Modern Art 1982)

O'Doherty M, *Internet Law* (1st edn, Bloomsbury Professional 2020

Patton M.Q, *Qualitative research and evaluation methods* (3rd edn, Thousand Oaks, CA: Sage, 2002)

Parahoo K, Nursing Research: Principles, Process and Issues (2nd edn, Basingstoke: Palgrave 2006)

Powell A, & Henry N, *'Sexual violence in a digital age'* (1st edn, Palgrave Macmillan, London 2017)

Rettberg J.W, *Seeing ourselves through technology: How we use selfies, blogs and wearable devices to see and shape ourselves* (Palgrave Macmillan 2014)

Rössler B, *The Value of Privacy* (Wiley, 2004)

Schiff Berman P, *Global Legal Pluralism: A Jurisprudence of Law Beyond Borders* (Cambridge University Press 2012)

Solove D, *The Future of Reputation: Gossip, Rumor and Privacy on the Internet* (Yale University Press 2007)

Sontag S, *On Photography* (New York: Picador 1977)

Staples W, *Everyday Surveillance: Vigilance and Visibility in Postmodern Life* (Lanham: Rowman & Littlefield 2013)

Suzor N, *Lawless: The Secret Rules that Govern our Digital Lives* (Cambridge University Press 2019)

Wallace P, *The Psychology of the Internet* (2nd edn, Cambridge University Press 2001)

Westin A, *Privacy and Freedom* (New York, Atheneum 1967)

Chapters in books

Bell J, 'Legal Research and the Distinctiveness of Comparative Law' in Mark Van Hoecke (ed) *Methodologies of Legal Research: Which Kind of Method for What Kind of Discipline?* (Bloomsbury Publishing Plc, 2011)

Bogner A, & Menz W, 'The Theory-Generating Expert Interview: Epistemological Interest, Forms of 39 Knowledge, Interaction' in A. Bogner & ors (eds.), *Interviewing Experts* (Palgrave and MacMillan, 2009)

Burns A, 'In full view: Involuntary porn and the postfeminist rhetoric of choice' in Claire Nally & Angela Smith (eds), *Twenty-first century feminism* (Palgrave Macmillan, London 2015)

Clayton R, Murdoch S, & Watson R, 'Ignoring the Great Firewall of China' In: Danezis G. and Golle P. (eds) *Privacy Enhancing Technologies* (PET 2006)

Coroneos P, 'Internet Content Policy and Regulation in Australia' in Kate Crawford and Catherine Lumby (eds), *The Adaptive Moment: A Fresh Approach to Convergent Media in Australia* (University of New South Wales 2011)

Cotterrell R, 'Comparative Law and Legal Culture' in Mathias Reimann and Reinhard Zimmermann (eds), *The Oxford Handbook of Comparative Law* (Oxford University Press 2006)

Dannemann G, 'Comparative Law: Study of Similarities or Differences?' in Mathias Reimann and Reinhard Zimmermann (eds), *The Oxford Handbook of Comparative Law* (Oxford University Press, 2006)

Denning D.E, and William E. Baugh W.E, 'Hiding crimes in cyberspace' in D. Thomas and B. D. Loader (eds), *CyberCrime: Law Enforcement, Security, and Surveillance in the Information Age* (Routledge 2000)

Eneman M, 'The New Face of Child Pornography' in M Klang and A Murrary (eds) *Human Rights in the Digital Age* (Routledge-Cavendish 2005)

Gómez Cruz E, & Miguel C, 'I'm Doing This Right Now and It's for You: The Role of Images in Sexual Ambient Intimacy' in M. Berry, & M. Schleser (eds) *Mobile Media Making in an Age of Smartphones* (New York: Palgrave Macmillan 2014)

Hardy S, 'The new pornographies: Representation or reality?' in Fiona Attwood (ed.) *Mainstreaming Sex: The Sexualization of Western* (IB Tauris & Co 2009)

Herodotus, 'The memos of Herodotus' in Robert Hutchins and George Rawlinson (eds), *Great Books of the Western World: Herodotus* (1952)

Holvast J, ‘History of Privacy’ in Vashek Matyas and others (eds), *The Future of Identity in the Information Society* (Springer 2009)

Jansen N, ‘Comparative Law and Comparative Knowledge’ in Mathias Reimann and Reinhard Zimmermann (eds), *The Oxford Handbook of Comparative Law* (Oxford University Press, 2006)

Lasén, A, ‘Autofotos. subjetividades y medios sociales’ [Selfies: Subjectivities and social media]. In García-Canclini N, & Cruces F, (eds.) *Jóvenes, culturas urbanas y redes digitales. Prácticas emergentes en las artes, el campo editorial y la música [Young people, urban cultures and digital networks. Emerging practices in arts, editorial field and music]* (Madrid: Ariel 2012)

Meuser M, & Nagel U, ‘The Expert Interview and Changes in Knowledge Production’ in A. Bogner & ors (eds.) *Interviewing Experts* (Palgrave and MacMillan, 2009)

Muncey T, ‘Does Mixed methods constitute a change in paradigm? In: Andrews, S; Halcomb, E eds. *Mixed Methods Research for Nursing and the Health Sciences*, 2009 (Chichester: Wiley Blackwell)

Pfitzmann A, & Köhntopp M, ‘Anonymity, Unobservability, and Pseudonymity – A Proposal for Terminology’ in Hannes Federrath (ed), *Designing privacy enhancing technologies* (Springer-Verlag 2001)

Powell A, Henry N, & Flynn A, ‘Image-based sexual abuse’ In W. S. DeKeseredy, C. M. Rennison, & A. K. Hall-Sanchez (eds.). *The Routledge International Handbook of Violence Studies* (New York: Routledge 2018)

Rachels J, ‘Why Privacy Is Important’ in Ferdinand David Schoeman (ed.) *Philosophical Dimensions of Privacy: An Anthology* (Cambridge University Press 1984)

Ritchie J, & Spencer L, ‘Qualitative data analysis for applied policy research’ in A.Bryman and R. G. Burgess (eds) *Analyzing qualitative data* (Routledge London, 1994)

Richie J, Spencer L, & O’Connor W, ‘Carrying out qualitative analysis’ in Jane Ritchie and Jane Lewis (eds) *Qualitative Research Practice: A Guide for Social Science Students and Researchers* (London: Sage 2003)

Salter M, & Crofts T, ‘Responding to revenge porn: Challenging online legal impunity’ in Comella, L. and Tarrant, S. (eds.) *New views on pornography: Sexuality, politics and the law* (Praeger Publisher: Westport 2015)

Scifo B, ‘The domestication of camera-phone and MMS communication. Early experiences of young Italians’ in K. Nyìri (ed.) *The global and the local in mobile communication* (Wien: Passagen Verlag 2005)

Stroud S, & Henson J, ‘Social media, online sharing and the ethical complexity of consent in revenge porn’ in A. Close (ed.), *Online Consumer Behavior: The Dark Side of Social Media* (United States: Routledge Press 2017)

Webley L, ‘Qualitative Approaches to Empirical Legal Research’ in P. Cane & H. Kritzer (eds) *The Oxford Handbook of Empirical Legal Research* (Oxford University Press, 2010)

Reports

Chertoff M, & Simon T, ‘The Impact of the Dark Web on Internet Governance and Cyber Security’ Global Commission on Internet Governance (Paper Series No. 6 — February 2015)

Children’s Rights Alliance, *Report Card 2021* (2021)

Franks M.A, *Drafting an Effective "Revenge Porn " Law: A Guide for Legislator* (Cyber Civil Right Initiative, 2 November 2015)

Gotsis T, *Revenge pornography, privacy and the law* (NSW Parliamentary Research Service — e-brief Issue 7/2015)

Henry N, Powell A, & Flynn A, *Not just ‘revenge pornography’: Australians’ experiences of image-based abuse: A summary report* (Melbourne: RMIT University 2017)

Henry N, Flynn A, & Powell A, ‘Responding to ‘revenge pornography’: Prevalence, nature and impacts’ Report to the Criminology Research Advisory Council Grant: CRG 08/15-16 (March 2019)

Jardine E, ‘The Dark Web Dilemma: Tor, Anonymity and Online Policing’ Global Commission on Internet Governance. (Paper Series No. 21 — September 2015)

Koontz L, ‘File Sharing Programs, Users of Peer-to-Peer Networks Can Readily Access Child Pornography’ (United States General Accounting Office Report GAO-03-1115T, 2003)

Kruithof K, Aldridge J, Décary Hétu D, Sim M, Dujso E, & Hoorens S, *Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands* (Santa Monica, Calif.: RAND Corporation, RR-1607-WODC, 2016)

Lasén A, *Understanding mobile phone users and usage* (Newbury: Vodafone Group R&D 2005)

Lenhart A, & Duggan M, *Couples, the Internet, and Social Media* (PEW Research Centre 202.419.4500 — February 2014)

Lenhart A, Ybarra M, & Price-Feeney M, *Online Harassment, Digital Abuse and Cyberstalking in America* (Report 11.21.16 Data and Society Research Institute)

McGlynn C, Rackley E, Johnson K, Henry N, Gavey N, Flynn A, Powell A, & Scott A, ‘Shattering lives and myths: A report on image-based sexual abuse’ (2019) *Project Report. Durham University; University of Kent*

National Research Council, Funding a Revolution: Government Support for Computing Research (National Academy Press 1999)

New Zealand Law Commission, Harmful digital communications: the adequacy of the current sanctions and remedies (Ministerial briefing paper, Wellington 2012)

Nyst C, *End Violence: Internet Intermediaries and Violence against Women Online* (Executive Summary and Findings, Association for Progressive Communications, July 2014)

OECD, Directorate for Science, Technology and Industry, Committee for Information, Computer and Communication Policy, The Role of Internet Intermediaries In Advancing Public Policy Objectives, Forging partnerships for advancing public policy objectives for the Internet economy, Part II (2011)

Office of the eSafety Commissioner, *Image-Based Abuse Qualitative Research Summary* (October 2017)

Office of the eSafety Commissioner, 'National Survey on image-based abuse in Australia' *Report prepared for the Office of the eSafety Commissioner* (Melbourne: RMIT University, 2017)

Powell A, & Henry N, *Digital Harassment and Abuse of Adult Australians, A Summary Report* (Melbourne: RMIT University, 2015)

Powell A, Henry N, Scott A & Flynn A, *Image-based sexual abuse: An international study of victims and perpetrators. Summary Repor*t (February 2020)

Rao J, & Rohatgi P, Can Pseudonymity Really Guarantee Privacy? (9th USENIX Security Symposium Paper 2000)

Smith, A, *15% of American adults have used online dating sites or mobile dating apps* (Washington, DC: Pew Research Center 202.419.4372 — February 2016)

UN Human Rights Council, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (2015) A/HRC/29/32

United Nations Committee, *Eighth Periodic Report on the Elimination of Discrimination against Women* (20 July 2018)

U.S. Department of Justice, *Cyberstalking: A New Challenge for Law Enforcement and Industry* (Washington, DC:GPO 1999)

Wittes B, Poplin C, Jurecic Q, & Spera C, 'Sextortion: Cybersecurity, teenagers, and remote sexual assault' (Centre for Technology Innovation at Brookings — May 2016)

Women's Aid, *One in Five Women Report, Experience Intimate Relationship Abuse Women's Aid 2020, TOO INTO you*

Newspaper reports

Alexander E, ‘Ugandan Pop Star Desire Luzinda could be Arrested over 'Revenge Porn' Nude Pictures’ *Independent* (12 November 2014)

Alter C, ‘‘It’s Like Having an Incurable Disease’: Inside the Fight Against Revenge Porn’ *Time U.S* (13 June 2017)

Bahadue N, ‘Victims of Revenge Porn Open Up on Reddit about How It Impacted Their Lives’, *Huffington Post* (New York, 10 January 2014)

Bardon S, ‘Upskirting’, cyberstalking, and revenge porn to be criminal offences’ *Irish Times* (Dublin, 15 May 2017)

Barker M, ‘Revenge Porn Is No Longer a Niche Activity Which Victimises Only Celebrities-The Law Must Intervene’ *Independent* (19 May 2013)

Bever L, ‘Fighting Back against Revenge Porn’ *Washington Post* (Washington, 28 April 2014)

Bowers S, ‘Government urged to outlaw creation and sharing of private sexual images’ *The Irish Times* (Dublin, 8 October 2019)

Buchanan R, ‘Jennifer Lawrence Nude Pictures Leak Sparks Fear of More Celebrity Hackings: A Flagrant Violation of Privacy’ *The Independent* (1 September 2014)

Burns S, ‘Dara Quigley case: inquiry under way into possible data breach’ *The Irish Times*, Dublin, 14 May 2017)

Clarke V, ‘Ask Facebook to leave Ireland if it won’t control content’ *Irish Times* (Dublin, 19 July 2018)

Courtney D, ‘There was nothing the guards could do for me’ - victim of revenge porn speaks out’ *Irish Independent* (Dublin, 27 September 2016)

Coyne E, ‘Varadkar axed digital safety officer plan after meeting Facebook’s Mark Zuckerberg’ *The Times* (Dublin, 2 August 2018)

Coyne E, ‘The cowardly backlash against women who discovered online campaign of image-based sexual abuse’ *The Independent* (Dublin, 20 November 2020)

D'Arcy C, ‘Labour publishes Bill to criminalise revenge porn’ *Irish Times* (Dublin, 4 April 2017)

Dent G, ‘The Case of Brenda Leyland and the McCanns is a thoroughly modern tale of internet lawlessness’ *The Independent* (Dublin, 6 October 2014)

Digital Desk ‘Warning over chilling impact on ‘freedom of expression’ if social media regulation unchecked’ *Irish Examiner* (Dublin, 6 April 2018)

Doyle k, ‘Facebook warns Digital Safety Commissioner 'could limit freedom of expression' *Independent* (Dublin, November 2018)

Duffy R, ‘Calls for fines and gardaí after undercover report about Facebook moderation in Dublin’ *The Journal* (18 July 2018)

Feehan C, ‘Garda who filmed tragic journalist Dara Quigley to avoid prosecution’ *The Irish Independent* (Dublin, 4 August 2018)

Gallagher C, ‘Garda who shared video of mentally ill woman will not face charges’ *The Irish Times* (Dublin, 7 August 2018)

Gallagher C, ‘Family of Dara Quigley yet to be contacted by Garda management’ *The Irish Times* (Dublin, 8 August 2018)

Gallagher C, ‘Garda pessimistic about bringing charges over ‘revenge porn’ leaks’ *The Irish Times* (Dublin, 21 November 2020)

Geiorgiev V, 'It made me feel really dirty' - Victim powerless against revenge porn attack’ *The Journal* (21 June 2016)

Graham-McLay C, Ramzy A, & Victor D, ‘Christchurch Mosque Shootings Were Partly Streamed on Facebook’ *New York Times* (New York, 14 March 2019)

Graham-McLay C, ‘Death Toll in New Zealand Mosque Shooting Rises to 51’ *New York Times* (New York, 2 May 2019)

Holland K, ‘Online proposals have no sanctions against service providers’ *Irish Times* (Dublin, 11 July 2018)

Holland K, ‘Dara Quigley’s family ‘battling State’ to find out key events before death’ *Irish Times* (Dublin, 23 October 2019)

James, O. ‘He’s clean bowled by a sick need for pleasure’ *Daily Telegraph* (2 July 2005)

Keate G, ‘Facebook Removes “Offensive’ Photo of Breastfeeding Mother’, *The Times* (London, 30 October 2014)

Keena C, ‘Staffing levels in new Media Commission expected to be similar to DPC office
Office’ *The Irish Times* (Dublin, 13 April 2021)

Lally C, ‘Gardaí have ‘limited scope’ on ‘revenge porn’’ *Irish Independent* (Dublin, 22 April 2015)

Loughlin E, ‘ISPCC: Child safety measures don’t go far enough’ *Irish Examiner* (Dublin, 30 March 2018)

Laville S, ‘Top tech firms urged to step up online abuse fightback’ *The Guardian* (11 April 2016)

Managh R, 'Twitter ordered to remove “defamatory” profile of Irish teacher' I*rish Times* (Dublin, 31 December 2013)

McCormack C, ‘Revenge porn nightmare: 'I felt I was completely violated'’ *Irish Independent* (Dublin, 12 June 2016)

McGoogan C, ‘Dark Web Browser Tor is Overwhelmingly Used for Crime, Says Study’ *The Telegraph* (London, 2 February 2016)

Moore A, ‘Assistant commissioner to lead urgent probe into intimate images leak’ *The Irish Examiner* (Dublin, 17 February 2021)

O’Connor R, ‘Gardaí say 'no evidence' sexual images of Irish women stolen’ *The Irish Post* (Dublin, 26 November 2020

O’Brien T, ‘Cyberbullying watchdog office should open without delay’ *Irish Times* (Dublin, 29 March 2018)

O’Halloran M, ‘Tánaiste ‘appalled’ at CCTV footage of Dara Quigley appearing online’ *The Irish Times* (Dublin, 11 May 2017)

O’Sullivan B, ‘Social media giants must be excluded from online safety watchdog role’ *Irish Times* (Dublin, 21 July 2018)

Pilkington Ed, ‘Tyler Clementi, Student Outed as Gay on Internet, Jumps to His Death’ *The Guardian* (London, 30 September 2010)

Reimer S, ‘Intimate Photos That Would Intimately’ *Baltimore Sun* (30 October 2013)

Roy J, ‘Revenge-Porn King Hunter Moore Indicted on Federal Charges’ *Time* (23 January 2014)

Ryan Ó, ‘Gardaí looking into allegations that large number of images of women were shared online without their consent’ (*The Journal*, 19 November 2020)

Samson A, ‘Dark Net May Pose ‘Disruptive Risk’ to Internet Sector—Goldman’ *Financial Times* (London, 13 July 2017)

Sankin A, ‘Revenge Porn: California Legislators Go After Troubling New Trend’ *Huffington Post* (San Francisco, 21 June 2013)

Sullivan G, ‘Ugandan Official Wants to Arrest Victim of Revenge Porn: 'She Should Be Locked up and Isolated'’ *Washington Post* (Washington, 12 November 2014)

The Associated Press, ‘California: Man Is Charged in 'Revenge Porn' Case’ *New York Times* (New York, 10 December 2013)

The Editorial Board, ‘The Discord Leak Was Harrowing. It Cannot Happen Again’ (*University Times*, 22 November 2020)

Thompson Don, ‘Court Date Set for Kevin Bollaert in Revenge Porn Website Case’ *Huffington Post* (12 December 2013)

Wahlquist C, ‘Christchurch shooting gunman intended to continue attacks, say PM’ (*The Guardian*,16 March 2019)

Whitehead T, ‘Twitter cases threat to freedom of speech’ *The Telegraph* (London, 3 February 2013)

Online Soucres

AAP, 'NSW Govt to Consider "Revenge Porn" Laws', (The Australian, 3 March 2016), < http://www.theaustralian.com.au/news/latest-news/let-revenge-porn-victims-sue-nswreport/news-story/e620808a31d2578c773627c9c3451257 > accessed 20 February 2022

Alexander L, 'Facebook's Censorship of Aboriginal Bodies Raises Troubling Ideas of 'Decency'', (*The Guardian*, 23 March 2016) < https://www.theguardian.com/technology/2016/mar/23/facebook-censorship-topless-aboriginal-women > accessed 20 February 2022

Australian Bureau of Statistics, 'Household Use of Information Technology, Australia, 2016- 17' < http://www.abs.gov.au/ausstats/abs@.nsf/mf/8146.0 > accessed 10 May 2018

Australian Bureau of Statistics, 'Australian Demographic Statistics' (2019) <https://www.abs.gov.au/AUSSTATS/abs@.nsf/DetailsPage/3101.0Mar%202019?OpenDocument> accessed 16 June 2020

Australian Communications and Media Authority, Parents' Guide to Online Safety <https://www.ideas.org.au/uploads/events/333/Parenting%20online.pdf> accessed 11 July 2020

Australian Communications and Media Authority, 'Who We Are' < https://www.acma.gov.au/who-we-are > accessed 4 July 2020

Bailey D, Brown D, Qurashi S, Loizou D, Rodgers L, & Shah P, 'Christchurch shootings: How the attacks unfolded' (BBC, 18 March 2019) < https://www.bbc.com/news/world-asia-47582183 > accessed 24 February 2022

BBC, 'Dark Net Guns Shipped in Old Printers' (BBC News, 20 July 2017) < https://www.bbc.com/news/technology-40668749 > accessed 16 February 2022

BBC News, 'Christchurch Shootings: 49 dead in New Zealand mosque attacks' (15 March 2019) < https://www.bbc.com/news/world-asia-47578798 > accessed 17 October 2020

Burleigh N, 'Sexting, Shame and Suicide' (*Rolling Stone*, 17 September 2013) <https://www.rollingstone.com/culture/culture-news/sexting-shame-and-suicide-72148/> accessed 20 February 2022

Cadwalladr C, 'Charlotte Laws' Fight with Hunter Moore, the Internet's Revenge Porn King' (*Guardian*, 30 March 2014) < https://www.theguardian.com/culture/2014/mar/30/charlotte-laws-fight-with-internet-revenge-porn-king > accessed 20 February 2022

Celada L, 'REALCORE Sergio Messina: The Margaret Mead of Internet Porn' (*Artillery*, January 2010), <http://www.artillerymag.com/archives/v4i3-l0/current/featurel.html > accessed 15 August 2017

Communications Alliance, 'Family Friendly Filters' < https://www.commsalliance.com.au/Activities/ispi/fff > accessed 6 Jan 2021

Council of Europe, 'Chart of signatures and ratifications of Treaty 185' <https://ccdcoe.org/organisations/council-of-europe/> accessed 10 January 2022

Cross-Tab, 'Online Reputation in a Connected World' (2010) <file:///C:/Users/emers/Downloads/DPD_Online%20Reputation%20Research_overview.pdf> accessed 20 February 2022

Cyber Civil Rights Initiative, 'End Revenge Porn Infographic' (2014) < https://www.cybercivilrights.org/wp-content/uploads/2014/12/RPStatistics.pdf > accessed 20 February 2022

Cyber Civil Rights Initiative, 'Non Consensual Porn: A Common Offence' (*Cyber Civil Rights Initiative*, 12 June 2017) <https://www.cybercivilrights.org/2017-natl-ncp-research-results/> accessed 4 March 2019

Cyber Cooperation Program < https://www.dfat.gov.au/international-relations/themes/cyber-affairs/cyber-cooperation-program/Pages/cyber-cooperation-program > accessed 24 February 2022

Cyber Safety Pasifika < https://www.cybersafetypasifika.org/our-work/latest-news/launch-new-cyber-safety-pasifika-program > accessed 24 February 2022

Data Protection Commissioner, 'Data Protection Commission statement on funding in 2021 Budget' (DPC, 13 October 2020) < https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-statement-funding-2021-budget > accessed 21 February 2022

Data Protection Commissioner, 'Data Protection Commission Statement on Budget 2022' (DPC, 12 October 2021) <https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-statement-budget-2022#:~:text=Commissioner%20Helen%20Dixon%20welcomes%20the,the%20Government%20in%20Budget%202022. > accessed 21 February 2022

DIGI, 'About DIGI' < https://digi.org.au/about/ > accessed 24 February 2022

Duffy R, 'Deplorable and revolting' treatment of deceased activist Dara Quigley is raised in the Dáil, (*The Journal*, 11 May 2017) < https://www.thejournal.ie/dara-quigley-dail-3384651-May2017/ > accessed 22 February 2022

Elliott S, 'Non–Consensually Shared Photography and the Need for Reform in Ireland' (2015) < https://acjrd.ie/images/PDFs/essay-competitions/Non-consensually_shared_pornography_and_the_need_for_reform_in_Ireland.pdf> accessed 20 February 2022

Farrell P, 'Inside the Darknet: Where Australians Buy and Sell Illegal Goods' (The Guardian, 4 July 2017) <https://www.theguardian.com/technology/2017/jul/04/inside-the-darknet-where-australians-buy-and-sell-illegal-goods> accessed 16 February 2022

Foxe K, 'Revealed: Data Protection Commission's pleas for more staff and 'fit-for-purpose' office; (The Journal, 12th October 2019) < https://www.thejournal.ie/data-protection-budget-4848807-Oct2019/ > accessed 21 February 2022

Fulbright Y.K, 'Scintillating Sexting' (Psychology Today, 14 September 2012) <https://www.psychologytoday.com/ie/blog/mate-relate-and-communicate/201209/scintillating-sexting> accessed 20 February 2022

Godfrey M, 'Revenge Porn Spreading like Wildfire', (*The Australian*, 22 November 2013) < http://www.theaustralian.com.au/news/latest-news/revenge-pornspreading-like-wildfire/story-fn3dxiwe-1226766034486 > accessed 20 February 2022

Gonzalez M, 'Power in Numbers' **(**Cyber Civil Rights Statistics on Revenge Porn, 3 January 2014) < https://cybercivilrights.org/revenge-porn-infographic/> accessed 14 January 2022

Halloran L, 'Race to Stop 'Revenge Porn' Raises Free Speech Worries' (NPR, 6th March 2014) < https://www.npr.org/sections/itsallpolitics/2014/03/06/286388840/race-to-stop-revenge-porn-raises-free-speech-worries?t=1645387722719 > accessed 20 February 2022

Hayes I, 'It made me feel really dirty' - Victim powerless against revenge porn attack' (*The Journal* 21 June 2016) < https://www.thejournal.ie/revenge-porn-irish-woman-no-legislation-2837138-Jun2016/ > accessed 20 February 2022

Henriksen M.A, 'Marilyn Monroe' (*American National Biography Online*, February 2000) <http://www.anb.orglarticles/18/18-00856.html.> accessed 15 August 2017

Hill K, 'Revenge porn with a Facebook twist' (Forbes, 6 July 2011) < https://www.forbes.com/sites/kashmirhill/2011/07/06/revenge-porn-with-a-facebook-twist/?sh=1abc8a2e1d2e > accessed 20 February 2022

Hill K, 'Why we find Hunter Moore and his "identity porn" site, IsAnyoneUp, so fascinating' (Forbes , 5 April 2012) < https://www.forbes.com/sites/kashmirhill/2012/04/05/hunter-moore-of-isanyoneup-wouldnt-mind-making-some-money-off-of-a-suicide/?sh=e4ed0ef794be > accessed 20 February 2022

Hill K, 'How Revenge Porn King Hunter Moore Was Taken Down' (*Forbes*, 21 January 2014) < https://www.forbes.com/sites/kashmirhill/2014/01/24/how-revenge-porn-king-hunter-moore-was-taken-down/?sh=2a03e30948c0 > accessed 20 February 2022

Human Rights and Technology <https://tech.humanrights.gov.au/julie-inman-grant> accessed 15 December 2020

Hunt E, 'Victoria Leads Way in Piecemeal Approach to Outlawing Revenge Porn', (*The Guardian*, 5 September 2016) < https://www.theguardian.com/australianews/2016/sep/05/victoria-leads-way-in-piecemeal-approach-to-outlawing-revenge-porn > accessed 20 February 2022

INHOPE, Annual Report 2020 < https://inhope.org/media/pages/the-facts/download-our-whitepapers/annual-report/bb4dd3cdc3-1628156678/inhope-annual-report-2020.pdf> accessed 17 January 2022

Internet Policy Observatory, 'The Santa Clara Principles on Transparency and Accountability of Content Moderation Practices' (2019) < http://globalnetpolicy.org/research/the-santa-clara-principles-on-transparency-and-accountability-of-content-moderation-practices/ > accessed 3 March 2019

Ipsos MRBI, 'Social Networking Quarterly' (April 2016) <http://ipsosmrbi.com/wpcontent/uploads/2016/05/SN_Apr16.png . > accessed 4 March 2019

Jacobs H, 'A Message from Our Founder' *(Cyber Civil Rights Initiative, 6 October 2013)* <http://www.cybercivilrights.org/amessagefromour_founderdrholly_.jacobs > accessed 4 March 2019

Johnston B, 'Privacy no longer a social norm, says Facebook founder' (*The Guardian*,11 January 2010) < https://www.theguardian.com/technology/2010/jan/11/facebook-privacy > accessed 20 February 2022

Keller D, "Final Draft of Europe's 'Right to be Forgotten' Law" (The Center for Internet and Society, Stanford Law School, 17 December 2015) < http://cyberlaw.stanford.edu/blog/2015/12/final-draft-europes-right-be-forgotten-law > accessed 20 February 2022

Leshnoff J, Sexting Not Just for Kids, (AARP, June 2011) < http://www.aarp.org/relationships/love-sex/info-11-2009/sexting_not_ just_for_kids.html > accessed 20 February 2022

Mar B, 'How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read' <https://www.bernardmarr.com/default.asp?contentID=1438 >accessed 20 February 2022

McAfee, 'Lovers beware: scorned exes may share intimate data online' (2013) <www.mcafee.com/us/about/news/2013/q1/20130204-01.aspx >accessed 20 February 2022

McDermot S, Facebook urges against 'punitive' fines for firms who breach Government's new online safety laws (*The Journal*, June 2019) < https://www.thejournal.ie/facebook-submissions-irish-government-safety-act-4699145-Jun2019/ > accessed 24 February 2022

McDermott S, 'Internet companies who break online safety rules could be blocked in Ireland under new law' (*The Journal*, 10 January 2020) < https://www.thejournal.ie/online-safety-commissioner-proposed-law-4960340-Jan2020/ > accessed 22 February 2022

Megan Jr, 'Make revenge porn a criminal offence in Ireland' < https://www.change.org/p/irish-justice-department-make-revenge-porn-a-criminal-offence-in-ireland?recruiter=false&utm_source=share_petition&utm_medium=twitter&utm_camp

aign=psf_combo_share_initial&utm_term=petition_dashboard&recruited_by_id=d26ca6b0-293a-11eb-8940-8986c7b8fb9a > accessed 16 June 2020

Morris A, 'Hunter Moore: The most hated man on the internet' (Rolling Stone, 11 October 2012) < https://www.rollingstone.com/culture/culture-news/hunter-moore-the-most-hated-man-on-the-internet-184668/ > accessed 20 February 2022

OECD, 'The Economic and Social Role of Internet Intermediaries' (April 2010) <https://www.oecd.org/sti/ieconomy/44949023.pdf > accessed 20 February 2022

Office of the eSafety Commissioner, 'Annual Reports' < https://www.esafety.gov.au/about-us/corporate-documents/annual-reports> accessed 15 December 2020

Office of the eSafety Commissioner, 'Deal with sextortion' < https://www.esafety.gov.au/key-issues/image-based-abuse/take-action/deal-with-sextortion> accessed 15 August 2020

Office of the eSafety Commissioner, 'eSafety Women' < https://www.esafety.gov.au/women > accessed 8 September 2018

Office of the eSafety Commissioner, 'eSafety Trusted Providers' <https://www.esafety.gov.au/educators/trusted-providers/find-providers> accessed 15 August 2020

Office of the eSafety Commissioner, 'How to report IBSA' < https://www.esafety.gov.au/report/image-based-abuse> accessed 15 August 2020

Office of the eSafety Commissioner, 'Get help to removes images and video' <https://www.esafety.gov.au/key-issues/image-based-abuse/take-action/get-help-remove-images-video> accessed 15 August 2020

Office of the eSafety Commissioner, 'Impacts and Needs' <https://www.esafety.gov.au/about-us/research/image-based-abuse/impacts-needs> accessed 15 August 2020

Office of the eSafety Commissioner, 'ISP Blocking: facts and falsehoods' (24 March 2020) <https://www.esafety.gov.au/sites/default/files/2020-03/eSafety-ISP-Blocking-factsheet.pdf > accessed 21 July 2020

Office of the eSafety Commissioner, 'Our Legislative Functions' <https://www.esafety.gov.au/about-us/who-we-are/our-legislative-functions> accessed 15 June 2020

Office of the eSafety Commissioner. 'Our Purpose' < https://www.esafety.gov.au/about-us/what-we-do> accessed 4 August 2020

Office of the eSafety Commissioner, 'Sending nudes and sexting' < https://www.esafety.gov.au/key-issues/staying-safe/sending-nudes-sexting> accessed 15 August 2020

Office of the eSafety Commissioner, Twenty Years Fighting Child Sexual Abuse; < https://www.esafety.gov.au/newsroom/media-releases/twenty-years-fighting-child-sexual-abuse-online> accessed 17 January 2022

Office of the eSafety Commissioner, 'Virtual Classrooms' <https://www.esafety.gov.au/educators/virtual-classrooms > accessed 18 October 2020

Office of the eSafety Commissioner, 'What We Do' < https://www.esafety.gov.au/about-us/what-we-do > accessed 22 February 2022

Office of the eSafety Commissioner, ' Women In The Spotlight: How online abuse impacts women in their working lives' <https://www.esafety.gov.au/about-us/research/how-online-abuse-impacts-women-working-lives# > accessed 22 February 2022

Office of the eSafety Commissioner, 'Working with social media' < https://www.esafety.gov.au/about-us/consultation-cooperation/working-with-social-media> accessed 16 August 2020

O'Reilly T, 'What Is Web 2.0? Design Patterns and Business Models for the Next Generation of Software' (2003) < https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html> accessed 20 February 2022

Parliament of Australia, 'Chapter 2 Key issues' <https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Former_Committees/cybersafety/cybersafety/report/c02> accessed 4 June 2020

Parliament of Australia, 'Infosheet 22 - Political parties' <https://www.aph.gov.au/About_Parliament/House_of_Representatives/Powers_practice_and_procedure/00_-_Infosheets/Infosheet_22_-_Political_parties> accessed 15 July 2020

Penny J, 'Deleting revenge porn' (*Policy Options Politiques,* 1 November 2013) < https://policyoptions.irpp.org/fr/magazines/vive-montreal-libre/penney/ > accessed 20 February 2022

Rackley E, & McGlynn C, 'The law must focus on consent when it tackles revenge porn' (*The Conversation,* 23 July 2014) < https://theconversation.com/the-law-must-focus-on-consent-when-it-tackles-revenge-porn-29501 > accessed 24 February 2022

RTE News, 'Revenge Porn, Cyber Stalking to become illegal offences' < https://www.rte.ie/news/2016/1231/841957-revenge-porn-cyberstalking-bill/ > accessed 17 May 2017

Safe Sexting: No Such Thing < https://www.rutherfordschools.org/media/it/onlinesafety/sextingfacts.pdf> accessed 13 January 2022

Statista, 'Hours of video uploaded to YouTube every minute as of February 2020' < https://www.statista.com/statistics/259477/hours-of-video-uploaded-to-youtube-every-minute/ > accessed 20 February 2022

Statista, 'Number of daily active Facebook users worldwide as of 4th quarter 2021' < https://www.statista.com/statistics/346167/facebook-global-dau/#:~:text=With%20roughly%202.89%20billion%20monthly,most%20popular%20social%20network%20worldwide > accessed 20 February 2022

The Conversation < https://theconversation.com/profiles/alastair-macgibbon-19023> accessed 15 December 2020

The Irish Council for Civil Liberties, 'ICCL brings Dara Quigley case to Justice Committee' (22 October 2018) < https://www.iccl.ie/news/dara-quigley-justice-committee/ > accessed 16th June 2020

ThinkUKnow, < https://www.thinkuknow.org.au/ > accessed 24 February 2022

Twitter Public Policy, 'Expanding and building #TwitterTransparency, 5th April 2018' < https://blog.twitter.com/en_us/topics/company/2018/twitter-transparency-report-12.html > accessed 20 February 2022

Wall E, 'Gardai commit to investigate every report of image-based abuse' (Extra.ie, 17 December 2020) < https://extra.ie/2020/12/17/news/irish-news/gardai-image-based-sexual-abuse-priority?utm_source=twitter&utm_medium=Social&utm_campaign=SocialWarfare > accessed 22 February 2022

Woodley N, & Taylor J, 'Revenge porn civil penalties considered by Government to give victims faster access to justice' (*The World Today*, 23rd November 2016) <https://www.abc.net.au/news/2016-11-23/revenge-porn-civil-penalties-could-serve-quicker-justice/8050054> accessed 17 July 2020

Woods L, & McGlynn C, 'Pornography platforms, the EU Digital Services Act and Image-Based Sexual Abuse' (*Media@LSE blog*, 26 January 2022) < https://blogs.lse.ac.uk/medialse/2022/01/26/pornography-platforms-the-eu-digital-services-act-and-image-based-sexual-abuse/ > accessed 25 February 2022

Zemler E, 'Naked & Famous: How a Risque New Website Pushes Boundaries and Buttons' (14 February 2011) <http://www.altpress.com/features/entry/naked-famous-how_a-risque-new website-pushes boundaries and buttons.> accessed 4 March 2019

Official reports (Ireland)

Government of Ireland, *Action Plan for Online Safety 2018-2019*

Houses of the Oireachtas, Joint Committee on Children and Youth Affairs, *Report on Cyber Security for Children and Young Adults* (32 CYA 011 — March 2018)

Law Reform Commission, *Harmful Communications and Digital Safety* (LRC 116 — 2016)

The Law Reform Commission, *Report on Regulatory Powers and Corporate Offences* (LRC 119-2018)

Irish Policy Material

Department of Communications, Climate Action and Environment, 'Open Policy Debate Online Safety' (Royal Hospital Kilmainham, 6 March 2018)

Department of Communications, *Climate Action & Environment, Public Consultation on the Regulation of Harmful Content on Online Platforms and the Implementation of the Revised Audiovisual Media Services Directive*

Department of Communications, *Climate Action & Environment, Public Consultation on the Regulation of Harmful Content on Online Platforms and the Implementation of the Revised Audiovisual Media Services Directive Explanatory Note*

Department of Communications, Climate Action & Environment, *Thematic Analysis - Public Consultation on the Regulation of Harmful Online Content and the Transposition of the Audiovisual*

Department of Communications and the Arts, Civil penalties regime for non-consensual sharing of intimate images (Discussion Paper May 2017)

Department of Justice, 'Private Member's Bill - Harassment, Harmful Communications and Related Offences Bill 2017' (9 August 2021) <https://www.gov.ie/en/speech/a85138-private-members-bill-harassment-harmful-communications-and-related-o/> accessed 24 January 2022

Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media, 'Regulation of Harmful Online Content and the Implementation of the revised Audiovisual Media Services Directive' (6 September 2020) < https://www.gov.ie/en/consultation/430d0-regulation-of-harmful-online-content-and-the-implementation-of-the-revised-audiovisual-media-services-directive/> accessed 22 February 2022

Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media, 'Minister Martin presents additions to new law proposed for online safety and media regulation' (Press Release, 9 December 2020)

Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media, 'Online Safety and Media Regulation Bill – Minister Catherine Martin proposes additional measures to assist community broadcasters, public service media and the radio sector' (Press release, 18 May 2021)

Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media , 'Publication of Online Safety and Media Regulation Bill '(12 January 2022) < https://www.gov.ie/en/speech/a175a-publication-of-online-safety-and-media-regulation-bill/> accessed 24th January 2022

Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media, 'Minister Martin presses forward with vital online safety law to establish new regulator' < https://www.gov.ie/en/press-release/528c3-minister-martin-presses-forward-with-vital-online-safety-law-to-establish-new-regulator/> accessed 8 February 2022

Government of Ireland, *Expert Group on an online safety individual complaints mechanism*, Terms of reference

Government of Ireland, General Scheme of the Online Safety and Media Regulation Bill Q&A

Government of Ireland, Online Safety and Media Regulation Bill, Annex to the Regulatory Impact Analysis

Government of Ireland, Online Safety and Media Regulation Bill, Summary of the virtual workshop on the regulatory framework for online safety (18 June 2020)

Government of Ireland, Regulatory Impact Assessment, Online Safety and Media Regulation Bill (November 2020)

Helen McEntee, Harassment, Harmful Communications and Related Offences Bill 2017: Committee Stage (1 December 2020)

Houses of the Oireachtas, Joint Committee on Children and Youth Affairs, *Report on Cyber Security for Children and Young Adults* (32 CYA 011 — March 2018)

Houses of the Oireachtas, 'Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht seeks stakeholder and expert submissions on Online Safety and Media Regulation Bill 2020' (11 February 2021) < https://www.oireachtas.ie/en/press-centre/press-releases/20210211-joint-committee-on-media-tourism-arts-culture-sport-and-the-gaeltacht-seeks-stakeholder-and-expert-submissions-on-online-safety-and-media-regulation-bill-2020/ > accessed 22 February 2022

Houses of the Oireachtas, Joint Committee on Tourism, Culture, Arts, Sport and Media debate, General Scheme of the Online Safety and Media Regulation Bill: Discussion (Resumed) (14 July 2021) <https://www.oireachtas.ie/en/debates/debate/joint_committee_on_tourism_culture_arts_sport_and_media/2021-07-14/3/?highlight%5B0%5D=online&highlight%5B1%5D=safety&highlight%5B2%5D=media&highlight%5B3%5D=regulation&highlight%5B4%5D=bill > accessed 22 February 2022

Irish Government News Service, 'Naughten hosts Government's Open Policy Debate on Digital Safety' < https://merrionstreet.ie/en/news-room/releases/naughten_hosts_government%E2%80%99s_open_policy_debate_on_digital_safety.html> accessed 24 January 2022

Joint Committee on Communications, Climate Action and Environment, Moderation of violent and harmful material on the Facebook platform: Discussion (1 August 2018)

Joint Committee on Tourism, Culture, Arts, Sport and Media, *Report of the Joint Committee on the Pre-Legislative Scrutiny of the General Scheme of the Online Safety and Media Regulation Bill* (TCASM/21/07 — November 2021)

Labour Admin, 'Howlin speech at launch of Harassment, Harmful Communications and Related Offences Bill 2017' < https://labour.ie/news/2017/04/04/howlin-speech-at-

launch-of-harassment-harmful-communications-and-related-offences-bill-2017/ > accessed 24 January 2022

Victoria State Government, 'Penalties and values' <https://www.justice.vic.gov.au/justice-system/fines-and-penalties/penalties-and-values> accessed 24 February 2022

Irish Submissions

Children's Rights Alliance, Submission to the Joint Oireachtas Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht on the General Scheme of the Online Safety and Media Regulation Bill (8 March 2021)

Facebook Ireland Limited, Public Consultation on the Regulation of Harmful Content on Online Platforms and the Implementation of the revised Audiovisual Media Services Directive (27 June 2019)

Farries E, Ansbro D, & Tierney G, 'The Irish Council for Civil Liberties Online Harassment Submission' to the Joint Committee on Justice and Equality (6 October 2019)

Irish Council of Civil Liberties, ICCL submission on the Online Safety and Media Regulation Bill To: Oireachtas Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht Date (8 March 2021)

Irish Council of Civil Liberties, ICCL submission to Pre-legislative scrutiny of the General Scheme of the Online Safety and Media Regulation Bill, Submission to the Joint Oireachtas Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht (26 May 2021)

Irish Human Rights and Equality Commission, Submission to the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht on the General Scheme of the Online Safety and Media Regulation Bill (March 2021)

Law Society of Ireland, Submission on the General Scheme of the Online Safety and Media Regulation Bill, Oireachtas Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht (18 March 2021)

Ombudsman for Children, General Scheme of the Online Safety and Media Regulation Bill 2020, Submission by the Ombudsman for Children's Office to the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht (4 March 2021)

Rory Coveney, Director of Strategy RTÉ, 'Online Safety and Media Regulation Bill Opening Statement ' <2021-05-20_opening-statement-rory-coveney-director-of-strategy-rte_en (1).pdf> accessed 22 February 2022

Submissions of Digital Rights Ireland to *Issues Paper on Cyber-crime Affecting Personal Safety, Privacy and Reputation Including Cyber-bullying* (2015)

Technology Ireland, submission on the General Scheme of the Online Safety and Media Regulation Bill (8 March 2021)

The Institute for Future Media, Democracy and Society (FuJo) and the National Anti-Bullying Research, The general scheme of the online safety and media regulation bill

submission to the joint committee on media, tourism, arts, culture, sport and the gaeltacht (March 2021)

Women's Aid, Submission to the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht on the General Scheme of the Online Safety and Media Regulation Bill (March 2021)

Irish Parliamentary Debates

Dáil Eireann Debate, 'Digital Safety Commissioner Bill 2017: Second Stage [Private Members]' (22 February 2018) < https://www.oireachtas.ie/en/debates/debate/dail/2018-02-22/30/#s33 > accessed 27 August 2018

Dáil Éireann Debate, 'Proposed Legislation' (4 July 2019) < https://www.oireachtas.ie/en/debates/question/2019-07-04/50/ > accessed 22 February 2022

Dáil Éireann Debate, 'Online Safety' (17 December 2020) < https://www.oireachtas.ie/en/debates/question/2020-12-17/319/> accessed 22 February 2022

Dáil Éireann Debate 'Online Safety' (15 June 2021) < https://www.oireachtas.ie/en/debates/question/2021-06-15/540/?highlight%5B0%5D=media&highlight%5B1%5D=online&highlight%5B2%5D=safety&highlight%5B3%5D=media&highlight%5B4%5D=regulation&highlight%5B5%5D=bill&highlight%5B6%5D=online&highlight%5B7%5D=online#pq-answers-540_541 > accessed 22 February 2022

Dáil Éireann Debate, Joint Committee on Tourism, Culture, Arts, Sport and Media debate, General Scheme of the Online Safety and Media Regulation Bill: Discussion (Resumed) (14 July 2021) < https://www.oireachtas.ie/en/debates/debate/joint_committee_on_tourism_culture_arts_sport_and_media/2021-07-14/3/?highlight%5B0%5D=online&highlight%5B1%5D=safety&highlight%5B2%5D=media&highlight%5B3%5D=regulation&highlight%5B4%5D=bill> accessed 22 February 2022

Australian Policy Materials

Australian Communications and Media Authority, Annual Report 2008/09

Australian Communications and Media Authority, *Communications Report* (2014-15)

Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2015/16

Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2016/17

Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2017/18

Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2018/19

Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2019/20

Australian Communications and Media Authority, Office of the eSafety Commissioner, Annual Report 2020/21

Australian Government Department of Communications, Enhancing Online Safety for Children Public consultation on key election commitments (January 2014)

Australian Government Department of Communications and the Arts, Civil penalties regime for non-consensual sharing of intimate images (Discussion paper, May 2017)

Australian Government Department of Communications and the Arts, Review of the Enhancing Online Safety Act 2015 and the Online Content Scheme – discussion (June 2018)

Australian Government Department of Communications and the Arts, Fact Sheet – Online safety reform proposal – Harmful online content (11 December 2019)

Australian Government Department of Communications and the Arts, Online Safety Legislative Reform Discussion Paper (December 2019)

Australian Government, Department of Infrastructure, Transport, Regional Development and Communications, 'Civil penalty regime for non-consensual sharing of intimate images' (Submissions) < https://www.infrastructure.gov.au/have-your-say/civil-penalty-regime-non-consensual-sharing-intimate-images > accessed 24 February 2022

Australian Parliament Joint Select Committee on Cyber-safety, *High-wire act: Cyber-safety and the young, interim report* (Canberra, Australia: Commonwealth of Australia 2011 — 146)

Australian Law Reform Committee, *Principled Regulation Federal Civil and Administrative Penalties in Australia* (Report 95 — December 2002)

Australian Law Reform Commission, *Classification — Content Regulation and Convergent Media* (Report 118 — 2012)

Australian and New Zealand Ombudsman Association, 'Peak body seeks to halt the misuse of the term Ombudsman' (*Media Release*, 18 May 2010)

Briggs L, *Report of the Statutory Review of the Enhancing Online Safety Act 2015 and the Review of Schedules 5 and 7 to the Broadcasting Services Act 1992 (Online Content Scheme)* October 2018

Department of Infrastructure, Transport, Regional Development and Communications, 'Consultation on a Bill for a new Online Safety Act' <

www.communications.gov.au/have-yoursay/consultation-bill-new-online-safety-act > accessed 26 February 2021

Department of Infrastructure, Transport, Regional Development and Communications, 'Consultation on Online Safety Reforms', < www.communications.gov.au/have-yoursay/consultation-online-safety-reforms > accessed 26 February 2021

Fletcher P, Minister for Communications, Cyber-Safety and the Arts, Second Reading Speech: Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Bill 2018 <https://www.paulfletcher.com.au/parliamentary-speeches/second-reading-speech-enhancing-online-safety-non-consensual-sharing-of > accessed 12 July 2020

Senator the Hon Mitch Fifield, Minister for Communications, 'New online reporting tool to tackle non-consensual sharing of intimate images' (Joint Media Release, 28 October 2016) < https://www.mitchfifield.com/2016/10/new-online-reporting-tool-to-tackle-non-consensual-sharing-of-intimate-images/ > accessed 24 February 2022

Senator the Hon Mitch Fifield, Minister for Communications, 'New reviews of online safety for Australians', (Media Release, 26 June 2018)

Law Reform Committee, Parliament of Victory, 'Inquiry into Sexting' *Report of the Law Reform Committee for the Inquiry into Sexting* (Parliamentary Paper No. 230, Session 2010-2013)

Notice of Indexation of the Penalty Unit Amount Federal Register of Legislation (Australia) 14 May 2020

Office of the eSafety Commissioner, *eSafety Regulatory Posture and Regulatory Priorities 2021-22* (November 2021)

The Coalition's Discussion Paper on Enhancing Online Safety for Children (November 2012)

The Coalition's Policy to Enhance Online Safety for Children (September 2013)

The Senate, Legal and Constitutional Affairs References Committee, *Phenomenon colloquially referred to as 'revenge porn'* (February 2016)

Australian Submissions

Alannah & Madeline Foundation, 'Response to the review into the Enhancing Online Safety Act 2015 and the Online Content Scheme' (August 2018)

Australian Government, 'Reviews of the Enhancing Online Safety Act 2015 and the Online Content Scheme' < https://www.infrastructure.gov.au/have-your-say/reviews-enhancing-online-safety-act-2015-and-online-content-scheme > accessed 20 February 2022

Berg C, 'Submission to the Senate Standing Committee on Environment and Communications Inquiry into Enhancing Online Safety for Children Bill 2014 and the

Enhancing Online Safety for Children (Consequential Amendments) Bill 2014' (January 2015)

Communications Alliance and the Australian Mobile and Telecommunications Association, 'Submission to the Department of Communications and the Arts Reviews of the Enhancing Online Safety Act 2015 and the Online Content Scheme – discussion paper' (25 July 2018)

Department of Home Affairs, 'Review of the Enhancing Online Safety Act 2015 and the Online Content Scheme' (August 2018)

Digital Industry Group Inc (DIGI), 'DIGI Submission to the review of the Enhancing Online Safety Act 2015' (August 2018)

Electronic Frontiers, Submission, Content Regulation in the Digital Age (2 February 2018) < https://www.ohchr.org/Documents/Issues/Opinion/ContentRegulation/EFF.pdf> accessed 20 February 2022

Office of the eSafety Commissioner, 'Submission: Review of the Enhancing Online Safety Act 2015 and the Online Content Scheme' (2018)

Third A, 'Submission to the Review of the Enhancing Online Safety Act 2015 and the Online Content Scheme' (2018)

Women in Media, 'Review of the Enhancing Online Safety Act -Submission' (July 2018)

EU Policy Material

Data Protection Working Party Opinion 5/2009 on online social networking 01189/09/EN WP 163 (June 2009)

European Commission, 'A Digital Single Market Strategy for Europe' Communication 192 final (6 May 2015)

European Commission, *Public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy* (24 September 2015)

European Commission, 'Online platforms and the Digital Single Market — Opportunities and Challenges for Europe' Communication 288/2 (25 May 2016)

European Commission, 'Proposal for a Directive amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audio-visual media services in view of changing market realities' Communication 287 final (25 May 2016)

European Commission, 'Proposal for a Directive on copyright in the Digital Single Market' Communication 593 final (14 September 2016)

European Commission, 'Tackling Illegal Content Online - Towards an enhanced responsibility of online platforms' Communication 555 final (28 September 2017)

European Commission, 'Guidance on certain aspects of Directive 2004/48/EC of the European Parliament and of the Council on the enforcement of intellectual property rights' Communication 708 final (29 November 2017)

European Commission, 'Commission Recommendation on measures to effectively tackle illegal content online' Communication 1177 final (1 March 2018)

Conference papers

Etter B, 'The Forensic Challenges of E-Crime' (7th Indo-Pacific Congress on Legal Medicine and Forensic Sciences, Melbourne, 21 September 2001)

Kang R, Brown S, & Kiesler S, 'Why Do People Seek Anonymity on the Internet? Informing Policy and Design' (Changing Perspectives Conference, Paris, April 2013)

Other

Channel 4 Dispatches, 'Inside Facebook: Secrets of the Social Network' (17 of July 2018)

Table of cases

Domestic cases

Glynn v Minister for Justice, Equality and Law Reform [2014] IEHC 133

Norris v Attorney General [1984] IR 36

McGee v Attorney General [1974] IR 284

Mosley v News Group Newspapers Limited [2008] EWHC 1777

Purcell v. Central Bank [2016] IEHC 514

X v Twitter [2011] EWHC 3454

European Cases

Ahmet Yildirim v Turkey (App No 3111/10) 18 December 2012

Bodil Lindqvist v Åklagarkammaren i Jönköping (C-101/01) [2004] ECR I 12971

Delfi v Estonia Application No 64569/09, ECtHR, 16 June 2015

Google France v Louis Vuitton Malletier SA and others (2010) ECLI:EU:C:2010:159

L'Oréal SA and others v eBay International AG and others (2011) ECLI:EU:C:2011:474

Google Spain SL v Gonzalez, No. C-131/12 (Court of Justice of the European Union May 13, 2014)

Nitecki v Poland Application No. 65653/01 21 March 2002

Odievre v France Application no. 42326/98, Judgment 13 February 2003.

Pretty v the UK (2002) 35 EHRR

Sentges v The Netherlands Application No. 27677/02 8 July 2003

S.S. 'Lotus', France V Turkey, Judgement, (1927) PCIJ Series A no 10, ICGJ 248.

Times Newspapers Ltd (Nos. 1 and 2) v United Kingdom [2009] (App Nos 3002/03 and 23676/03)

Tysiac v Poland Application no. 5410/03 Judgment 20 March 2007

Cases of other jurisdictions

A.H. v. State, 949 So. 2d 234, 237 (Fla. Dist. Ct. App. 2007) (United States)

Amicus Curiae v Microsoft [1999] D.D.C Civ 98 (United States)

Handyside v United Kingdom (1979-1980) 1 EHRR 737 (United Kingdom)

Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231,235 (Minn. 1998) (United States)

Laskey and Ors v. The United Kingdom (1997) 24 EHRR 39 (United Kingdom)

Miller v. Skumanick, 605 F. Supp. 2d 634 (M.D. Pa. 2009) (No. 3:09cv540) (United States)

Pub. Utilities Comm'n v. Pollak, 343 U.S. 451, 467 (1952) (United States)

Twentieth Century Music Corp. v. Aiken, 422 U.S. (1975) (United States)

Welsh v. Martinez, 144 A. 3d 1231 (Conn. App. Ct. 2015) (United States)

Wilson v Ferguson [2015] WASC 15 (Australia)

Wood v Hustler Magazine [1984] 736F.2D 1084 (5th Cir.) (United States)

Table of Legislation

Irish Legislation

Copyright and Related Offences Act 2000

Data Protection Act 2018

Defamation Act 2009

Digital Safety Commissioner Bill 2017

Draft Harmful Communications and Digital Safety Bill 2016

General Scheme of the Online Safety and Media Regulation Bill

Harassment, Harmful Communications and Digital Safety Bill 2017

Harassment, Harmful Communications and Related Offences Bill 2017

Harassment, Harmful Communications and Related Offences Act 2020

Non – Fatal Offences Against the Persons Act 1997

The Irish Constitution, article 40.3.1.

The Online Safety and Media Regulation Bill 2022

Australian Legislation

Classification (Publications, Films and Computer Games) Act 1995 (Federal)

Crimes Act 1900 (Australian Capital Territory)

Crimes Act 1900 (New South Wales)

Crimes Act 1958 (Victory)

Crimes Amendment (Sexual Offences and Other Matters) Act 2014 (Victory)

Criminal Code Act 1899 (Queensland)

Criminal Code Act 1924 (Tasmania)

Criminal Code Act 1983 (Northern Territory)

Criminal Code Act Compilation Act 1913 (Western Australia)

Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019 (Federal)

Criminal Code Amendment Bullying Act 2019 (Tasmania)

Criminal Law Consolidation Act 1935 (South Australia)

Enhancing Online Safety for Children Act 2015 (Federal)

Enhancing Online Safety Act 2015 (Federal)

Enhancing Online Safety (Family and Domestic Violence) Legislative Rules 2015 (Federal)

Enhancing Online Safety for Children Amendment Bill 2017 (Federal)

Enhancing Online Safety (Intimate Images and Other Measures) Legislative Rules 2017 (Federal)
Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Bill 2018 (Federal)
Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018 (Federal)
National Classification Code (May 2005) (Federal)
Online Safety Act 2021 (Federal)
Regulatory Powers (Standard Provisions) Act 2014 (Federal)
Summary Offences Act 1953 (South Australia)
The Broadcasting Services Amendment (Online Services) Act 1999 (Federal)
The Criminal Code Act 1995 (Federal)

Legislation of other jurisdictions

Anti-Photo and Video Voyeurism Act 2009 (Philippians)
Audiovisual Media Services Directive) [2010] OJ L 95/1 (European Union)
Charter of Fundamental Rights of the European Union 2000/C 364/01 (European Union)
Communications Decency Act 1996 (United States)
Council of Europe, Recommendation CM/Rec (2007)16 (European Union)
Digital Copyright Directive 2019 (European Union)
Directive on Electronic Commerce) 2000/31/EC OJ L 178/1 (European Union)
Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities. (European Union)
E-Commerce Directive 2000/31/EC (European Union)
Harmful Digital Communications Bill, 2013 (New Zealand)
The Digital Markets Act (European Union)
The Digital Services Act (European Union)
The General Data Protection Regulation 2016/679 (European Union)

Appendix A: Ethical approval Letter

MAYNOOTH UNIVERSITY RESEARCH ETHICS COMMITTEE

MAYNOOTH UNIVERSITY,

MAYNOOTH, CO. KILDARE, IRELAND

Maynooth University
National University of Ireland Maynooth

Dr Carol Barrett
Secretary to Maynooth University Research Ethics Committee

09 November 2018

Emer Shannon
Department of Law
Maynooth University

RE: Application for Ethical Approval for a project entitled: The global problem of image-based sexual abuse considered in the Irish context: An evaluation of existing legal responses with a focus on effective enforcement in the online environment, including through intermediary intervention

Dear Emer,

The Ethics Committee evaluated the above project and we would like to inform you that ethical approval has been granted.

Any deviations from the project details submitted to the ethics committee will require further evaluation. This ethical approval will expire on 31 December 2019.

Kind Regards,

Dr Carol Barrett

Secretary,

Maynooth University Research Ethics Committee

C.c. Dr Maria Helen Murphy, Department of Law, Maynooth University.

Reference Number
SRESC-2018-101

Appendix B: Interview information sheet and consent form
Participant Information Guidelines

Researcher: Emer Shannon

Supervisor: Dr Maria Helen Murphy

Institution: Department of Law, Maynooth University, Ireland

1. Introduction

My name is Emer Shannon, a doctoral student in the Department of Law at Maynooth University. I am undertaking a research study under the supervision of Dr Maria Helen Murphy as part of my doctoral research funded by the Law Department at Maynooth University.

You are invited to take part in this research project because you have been identified as a key actor pertaining to issues of online regulation.

This study seeks to assess the potential role of 'enforcers' – both private and state sanctioned – to provide adequate redress for victims of image-based sexual abuse in Ireland. Currently Ireland's Law Reform Commission have proposed a Digital Safety Commissioner to combat the posting of harmful content online which is based on a comparable office in Australia called the eSafety Commissioner. An analysis of the remediating powers of this body will provide an informed discussion of the potential effect of the proposed Digital Safety Commissioner in remedying victims of image-based sexual abuse and the potential role of online intermediaries in Ireland.

These Participant Information Guidelines establish the objectives and parameters of the research project. They explain what is involved to help you decide if you want to take part. Please read this information carefully and ask questions about anything you do not understand, require clarification on, or want to know more about.

Participation in this research is voluntary. If you decide to take part in the research project, please sign the consent form on page four. By signing the consent form you are confirming that you understand what you have read and that you consent to be part of the research project. Consent can be withdrawn at any stage during your participation either during the interview or after but before the submission of the final thesis in September 2020.

2. What is the purpose of the research project?

This research is being conducted as part of the researcher's PhD thesis. As technology and social media increasingly infiltrate daily life, the sharing of intimate images without consent known as image-based sexual abuse – commonly known as 'revenge pornography' – has become a significant issue. While the concept of image-based sexual abuse is not a new phenomenon, its spread has been adapted and facilitated by

advances in technology and the evolution of relationships in the 21st century. As reform efforts continue, enforcement challenges remain, and the debate on intermediary responsibility has exploded. Various approaches have been adopted internationally, yet academic consideration of the issue in the Irish context is minimal. This research aims to address that gap by deriving lessons from the common law jurisdiction of Australia that has legislated on this issue and established a regulatory body – the 'eSafety Commissioner'. This study seeks to gain insight into the functioning of the eSafety Commissioner in practice.

3. What does participation in this research involve?

Participation involves a single interview with the researcher lasting between thirty minutes and one hour in duration. In some instances, however, the interview may exceed this if the interview subject wishes to continue. The interview will take place at a time and venue of the participant's choosing or via Skype. The interview will be audio recorded. As stated further below in section 5, these interview audio recordings will be deleted once they have been transcribed. You will not be paid for your participation in this research.

4. How will I be informed about the final results of this research project?

The research will be published as a PhD thesis and may also form part of other academic publications by the researcher. All PhD theses are made available online in an e-theses database available at: http://eprints.nuim.ie/ Subsequent publications will be deposited in the university's e-prints database which is open access also. A copy of the final thesis will be emailed to you.

5. What will happen to the information about me?

If you choose to be anonymised your identity will be protected by referring to you by a pseudonym. The identification key for these pseudonyms will be kept on a secure server at Maynooth University. The researcher and supervisor alone will have access to the file of names and pseudonyms. Personally identifiable data collected will be irreversibly anonymised by September 2020 after the final submission of the thesis. All interviews will be audio recorded and transcribed. Once transcription is completed the recording will be deleted and the transcript will be encrypted and kept on a secure server at Maynooth University. The transcript will be sent to you for your approval.

After a period of ten years following completion of the project all transcripts and electronic files together with the code to pseudonyms held by the researcher and supervisor will be deleted. Any paper record referencing the interview data will be shredded.

The results will be seen by the researcher, supervisor and examiners and be presented in the published thesis, academic publications and conferences.

What are the possible advantages and disadvantages?

The researcher does not envisage any disadvantages for participants taking part in this study. Benefits include; the opportunity to voice your opinion and professional experiences, contribute to a wider understanding of how the eSafety Commissioner functions, and contribute recommendations that would improve the manner in which the removal of online intimate images is regulated.

6. Does this project have approval?

The project is being carried out in accordance with the Maynooth University Research Ethics Policy. The ethical aspects of this project have been approved by the Maynooth University Research Ethics Committee in November 2018.

Further queries?

If you need any further information, please feel free to contact me.

Researcher Emer Shannon, BBL, Joint LLM,
Department of Law, New House, Maynooth University, Co. Kildare, Ireland.
emer.shannon.2013@mumail.ie

Supervisor Dr. Maria Helen Murphy,
Department of Law, New House, Maynooth University, Co. Kildare, Ireland.
maria.murphy@mu.ie

If during your participation in this study you feel the information and guidelines that you were given have been neglected or disregarded in any way, or if you are unhappy about the process, please contact the Secretary of the National University of Ireland Maynooth Ethics Committee at research.ethics@nuim.ie or +353 (0)1 708 6019. Please be assured that your concerns will be dealt with in a sensitive manner.

It must be recognised that, in some circumstances, confidentiality of research data and records may be overridden by courts in the event of litigation or in the course of investigation by lawful authority. In such circumstances the University will take all reasonable steps within law to ensure that confidentiality is maintained to the greatest possible extent

Informed Consent Form

Researcher: Emer Shannon

Supervisor: Dr Maria Helen Murphy

Institution: Department of Law, Maynooth University, Ireland

(Please tick the relevant answer)

The purpose and nature of the study has been explained to me verbally & in writing. I've been able to ask questions, which were answered satisfactorily.	
I am participating voluntarily.	
I give permission for my interview with Emer Shannon to be audio recorded	
I understand that I can withdraw from the study, without repercussions, at any time, whether that is before it starts or while I am participating.	
I understand that I do not have to answer all questions during the interview and can refuse to answer a y question if I feel uncomfortable.	
I understand that I can withdraw permission to use the data right up to the submission of the thesis.	
It has been explained to me how my data will be managed and that I may access it on request.	
I understand the limits of confidentiality as described in the information sheet	
I understand that my data may be used in further research projects and any subsequent publications if I give permission below:	

Please tick the appropriate box	**YES**	**NO**
I agree to quotation/publication of extracts from my interview		
I agree for my data to be used for further research projects		
I agree to be identified by my name		
I agree to be identified through my organisation's name		

NAME (PRINT) _____

SIGNATURE _____

DATE _____

Contact Details:

Researcher: Emer Shannon **email:** emer.shannon.2013@mumail.ie

Supervisor: Dr Maria Helen Murphy **email:** maria.murphy@mu.ie

If during your participation in this study you feel the information and guidelines that you were given have been neglected or disregarded in any way, or if you are unhappy about the process, please contact the Secretary of the National University of Ireland Maynooth Ethics Committee at research.ethics@nuim.ie or +353 (0)1 708 6019. Please be assured that your concerns will be dealt with in a sensitive manner.

For your information the Data Controller for this research project is Maynooth University, Maynooth, Co. Kildare. Maynooth University Data Protection officer is Ann McKeon in Humanity house, room 17, who can be contacted at ann.mckeon@mu.ie. Maynooth University Data Privacy policies can be found at https://www.maynoothuniversity.ie/data-protection.

If you would like to withdraw from this research at any point, please sign below and return this form to me at:

Emer Shannon

Department of Law,

New House,

Maynooth University,

Maynooth, Co. Kildare

Signature _____ Date _____