Irish Council for Civil Liberties
FOR ALL OUR RIGHTS. NO EXCEPTIONS.
50 YEARS
SINCE 1976.
Enforce

Maynooth University
National University of Ireland Maynooth

Protecting the 'Privacy' in Privacy-Enhancing Technologies: Lessons from Apple's NeuralHash Detection Proposal and Google's Privacy Sandbox

Report, March 2026

A report produced from a collaboration between Maria Helen Murphy (Maynooth University School of Law) and Kris Shrishak (Irish Council for Civil Liberties)[*]

Summary

Privacy-Enhancing Technologies (PETs) are often presented as tools that enable the free flow of data while protecting personal information. In practice, however, PETs often fall short on their promise of safeguarding privacy without limiting data use. When privacy is reduced to a narrow conception of confidentiality, the tools marketed to enhance privacy risk undermining protection and entrenching existing concentrations of power. Drawing on two high-profile attempts at real-world deployment that were ultimately discontinued, this report shows how current approaches to PETs can obscure important risks, and that PETs must be understood as one component of a wider, rights-based governance framework rather than a technical fix for privacy problems. Crucially, broad engagement with diverse interdisciplinary stakeholders is an essential part of the process. In a time of legislative flux, where 'simplification' in pursuit of innovation is prominent in policy discussions, the limitations of PETs as a catch-all 'solution' must be accurately understood. This is especially the case as ongoing debates on the very 'notion of personal data', as reflected in the EU Digital Omnibus proposals, have the potential to further emphasise technical protections based on concepts of identifiability at the expense of full consideration of privacy harms.[1]

Key Insights

- Privacy-Enhancing Technologies (PETs) have an important role to play in the protection of privacy, but must be evaluated against a broad human rights informed concept of privacy, not just confidentiality.
- Conventional threat models used in the design and evaluation of PETs are too narrow.
- PETs can be used to legitimise surveillance and enable 'privacy-washing'.
- While the protection of individual rights is vital, group and systemic harms must also be considered.
- In a time of legislative flux, 'simplification' proposals in the EU Digital Omnibus risk narrowing the notion of personal data in ways that privilege technical, identifiability-based framings over meaningful protection against privacy harms (including the collective harms highlighted in this report).

Terminology Note

For the purposes of this report, the term 'privacy' is used in an inclusive way that covers both privacy and data protection. Although the exact relationship between these concepts is debated, both are relevant to the design, implementation, and evaluation of Privacy-Enhancing Technologies (PETs), especially when these technologies operate across different legal jurisdictions.[2] Where a distinction is legally important, we indicate this in the text.

1 Why Privacy-Enhancing Technologies Matter

Despite the significant legal protection that privacy and data protection receive in jurisdictions around the world, the reality of modern data processing, data-driven governance, and the data economy means that privacy and the related right to protection of personal data have faced mounting pressure.[3] Outside the legal sphere, technologists have responded to privacy encroachments by contributing to the field of PETs. This response can be seen as a 'technological fix for a technological problem,' although we conceive of the challenge as a social problem.[4]

A common rationale behind the development and deployment of PETs is reducing risk and the need for trust in data sharing.[5] Notably, PETs have the potential to provide a layer of protection for the unseen or minor intrusions that legal bodies like courts and regulators rarely have the opportunity to consider.[6] This is important as minor intrusions can aggregate over time to cause significant collective harm and unnoticed or obscured intrusions can cause harm in insidious ways that a typical individual may not be able to identify or prove with evidence.

While some companies have sought to differentiate themselves in the marketplace with claims of being privacy-conscious, the privacy paradox suggests a limited capacity in wider society to choose services based on privacy concerns.[7] In the complex modern data-processing environment, a typical user does not have the capacity to adequately protect their own privacy.

Early PETs focused mainly on traditional encryption; this greatly restricted the ability to process and extract economic value from data. A more recent wave of 'privacy-preserving computation' tools (including homomorphic encryption, secure multi-party computation, and differential privacy) claim to provide privacy assurances – useful for compliance and trust purposes – while attempting to maintain the utility as that of non-PETs computation. These advanced PETs often operate as 'invisible infrastructure' unbeknownst to end-users who are neither expected to control nor even understand them.[8]

The promise of PETs such as homomorphic encryption, secure multi-party computation, and differential privacy is that they can retain the benefits of data processing while still protecting the underlying data from being revealed unnecessarily.[9] These PETs make it possible to analyse data from multiple sources without having to see the data. This would appear to be the ideal outcome from a 'privacy-by-design' perspective, where privacy can be preserved without preventing innovative data use. As might be expected, business interest in PETs is primarily motivated by business benefits, and this illustrates the catalysing effect of privacy and data protection regulation on business practice. For example, PETs can help businesses to exploit data for insight and profit while being able to point to their compliance efforts. With provider-side PETs, this can be about more than simply automating compliance with legal obligations, but can also create the business opportunity for additional processing that may not be possible otherwise, either due to legal restrictions or customer preferences.

However, due to the resource-intensive nature of modern PETs, in practice only a limited number of large corporations that control key digital infrastructure (operating systems, browsers, app stores, etc.) can realistically deploy them at scale. This has the potential to hinder the transparency, effectiveness, and control of PETs that may be problematic from a human rights perspective.

Policymakers and regulators, nevertheless, see enormous potential in these tools to facilitate compliance.[10] This perspective suggests that society can 'have its cake and eat it' by both keeping the business model while protecting privacy.[11] Indeed, data protection regulators such as the UK's Information Commissioner's Office (ICO), the Office of the Privacy Commissioner of Canada (OPC), and Spain's Agencia Española de Protección de Datos (AEPD), have released materials on PETs and their potential role in privacy protection.[12] At the European level, the European Data Protection Supervisor (EDPS) recommends that EU institutions 'foster the roll-out and adoption of privacy by design approaches and PETs in the EU and at the Member States' level'.[13] The European Union Agency for Cybersecurity (ENISA) describes PETs as 'building blocks' towards meeting the Article 25 GDPR obligations on data protection by design.[14] Notwithstanding these notable endorsements, it must be recalled that privacy is a complex and multifaceted concept and how it is defined has significant implications for the scope and chosen means of protection.

2 How PETs Narrow the Concept of Privacy

Defining privacy is a complex question and the precise meaning of privacy has been subject to many different interpretations. What the concept means in a legal sense varies by jurisdiction and understandings of the concept continue to evolve. An inclusive interpretation of the right has facilitated responsiveness to technological innovation. For example, the finding that the right to respect for private life is a 'broad term not susceptible to exhaustive definition' has enabled the European Court of Human Rights (ECtHR) to identify a wide range of surveillance technologies that 'interfere with the right to respect for private life'.[15] Furthermore, by recognising the persistence of a right to respect for private life in information compiled from the public domain, the ECtHR moves beyond the 'classical' interpretation of privacy as concealment.[16] It is maintained that a broad interpretation is necessary to ensure the protection of privacy and its underlying values.

PETs that operationalise a narrow conception of privacy risk undermining these broader protections, even while claiming to 'enhance' privacy. It is acknowledged, however, that this position creates challenges for those seeking to design technologies that are 'privacy compliant' in the narrow sense.The uncertainty of scope places pressure on the word 'privacy' in 'Privacy-Enhancing Technology'. But it also explains, at least in part, the interest in PETs and their related processes, which some claim can help translate difficult-to-pin-down concepts into actionable technical specifications. This has clear appeal from a practical perspective, particularly due to the limits of law in this space. But, it also instantiates a particular and narrow understanding of privacy.[17]

Approaching this from a dual-disciplinary perspective, the translation challenges in this space are clear. The comprehension gap that exists between technologists and legal experts regarding technology is often commented upon, yet there is no simple solution. While transparency and understanding of how data is used and protected are important goals, the mathematical complexity underpinning privacy-enhancing techniques creates a practical challenge for not only individual data subjects and legal experts, but also for a broad array of stakeholders (including developers, investors, and policymakers).[18] Even with significant strides being made in the investment in technological expertise in regulatory bodies and sincere engagement on these issues by legal experts, the challenge remains.

Advanced PETs such as secure multi-party computation and differential privacy address the requirement to engineer privacy into systems in different ways. The former aims to protect input privacy and the latter, output privacy. By engineering the requirement, these PETs treat privacy as a property of the data instead of the right of humans to be protected. In the context of input privacy, for example, the 'privacy requirement' is defined to be 'that nothing should be learned beyond what is absolutely necessary; more exactly, parties should learn their output and nothing else.'[19] In this context, 'privacy' is 'turned into something mathematically formalisable' equating privacy to 'variations of confidentiality'.[20] As a result of this, broader conceptions of privacy are 'de-emphasised and de-prioritised.'[21] The gap between the different fields underlines rather than removes the need for interdisciplinary assessment and for documentation that is intelligible beyond a narrow technical audience.

Considering the interpretive complexities the concepts of privacy and data protection continue to present despite extensive regulatory, judicial, and academic efforts, it is worth considering how the concepts of privacy and data protection have been translated into the practical realm. The techniques of PETs rely on addressing privacy threats. These threats are often modelled in terms of adversary power and threat models. While these models have been useful in the academic literature, they have been found wanting in deployment, including where models treat powerful platforms and nation states as trusted actors and not as potential adversaries. We provide two case studies to illustrate the risks of this approach.

3 Case Studies: Apple's NeuralHash Detection and Google's Privacy Sandbox

The two case studies discussed in this section, focusing on Apple's proposed Child Sex Abuse Material detection system and Google's Privacy Sandbox, were selected to illustrate some of the risks of PETs.

Case Study 1: Apple's NeuralHash Detection

A high-profile and widely criticised deployment of privacy-enhancing techniques was the effort by Apple to introduce a new hashing algorithm that intended to allow the detection of Child Sex Abuse Material (CSAM) on iCloud servers while preserving privacy in a manner defined by Apple. Many cloud storage providers scan for CSAM on unencrypted data on their servers, but in what was described as an effort to preserve privacy, the proposed Apple detection system would rely on a cryptographic process that would partly occur on the individual user's Apple device and partly on Apple's servers.[22] The Apple system dubbed NeuralHash would create identifiers through the on-device hashing of photos. These identifiers would then be compared with identifiers in the National Center for Missing and Exploited Children database. While put forth as a privacy-preserving solution that would help to tackle a societal problem of utmost importance, the system was criticised for its vulnerabilities to adversary attacks, its potential to create false positives, and its capacity to be used as a surveillance tool.[23]

Feedback from a diverse cohort of stakeholders led to the pausing and eventual abandonment of the plan.[24] The failed introduction illustrated the weakness in adopting a siloed approach to privacy-enhancing solutions. While the Apple system was successful in achieving the goals it set out to accomplish in the abstract and in enhancing privacy by its specifications, it did not account for the real-world environment where the technology could be abused by nefarious actors including States abusing power by targeting political opponents. The fact that Apple ultimately abandoned its plans illustrates the importance of the opportunity to object to such measures and to meaningfully interrogate changes to dominant technological infrastructure. The imperative for a broad and open-minded engagement is reflected in Apple's Director of User Privacy's re-evaluation following the decision not to proceed with the plan 'after extensive consultation with experts'.[25] In 2023, the Director maintained Apple's commitment to tackling CSAM, but concluded that Apple's approach to CSAM detection was not 'practically possible to implement without ultimately imperilling the security and privacy' of Apple users.[26] Despite this, companies like Apple continue to face pressure to undermine encrypted services and it is likely that similar scanning proposals will arise again as a result.[27]

Case Study 2: Google's Privacy Sandbox

A second example of a globally dominant company touting its privacy-enhancing measures is provided by Google and its Privacy Sandbox. After several years of testing and regulatory scrutiny, Google retired a range of its Privacy Sandbox advertising technologies which failed to gain sufficient adoption in the ad-tech ecosystem.[28] Critics had also warned that the system had security vulnerabilities and failed to adequately mitigate privacy risks.[29] A key part of Google's Privacy Sandbox that has been retired is the Google Topics API. The idea behind this was to enable the serving of 'interest-based advertising' informed by the 'topics' associated with your browsing in Chrome over defined time periods. While this approach reduces reliance on the use of third-party cookies, it still allows for extensive observation and prediction of user behaviour.

The branding of these efforts as 'privacy' could be reasonably described as 'privacy washing' as they retain behavioural prediction and targeting in a different form.[30] To call it privacy is to take a very narrow view of what privacy is; it is a view that ignores the function of privacy in society beyond the simple confidentiality of information. Pertinent, of course, to all matters relating to privacy is the question of power and unsurprisingly, Google's privacy approach would also consolidate its information advantage.[31] The context behind Google's privacy-enhancing efforts is provided by doubts about the compatibility of real-time bidding and targeted behavioural advertising with GDPR obligations.[32] Looking ahead, reforms proposed in the Digital Omnibus, including plans to ease cookie consent obligations and narrow the scope of personal data, could reduce regulatory friction for dominant ad-tech platforms like Google. This could incentivise compliance approaches viewing privacy as a technical design choice rather than a fundamental right constraining current business models.

Although the 'privacy-enhancing' efforts by Apple and Google discussed above may achieve their internally defined goals, labelling those achievements as 'privacy' is an unduly narrow representation of the concept.[33] The following section considers privacy and its underlying values and the relationship of this complex concept to power.

4 Systemic Risks: Power, Accountability, and the Limits of PETs

As noted above, in thinking about these types of challenges more broadly, it is impossible to ignore the role of power.[34] The individual is always at a huge power disadvantage in the modern data environment due to constant and enormously complex data collection and data processing. The opacity and complexity make it difficult not only for citizens and civil society to be cognisant of risks and to effectively challenge privacy harms but also for regulators to fulfil their duties and hold systems of data processing up to scrutiny. The lack of transparency and general understanding about the functioning of PETs creates a risk that privacy-preserving computation may become 'not just a technical but a technocratic solution' imposed on populations without consent.[35] This contrasts with early conceptions of Privacy-Enhancing Technologies – from the simplest examples of camera covers to quite sophisticated encryption software – which often acted as beacons of empowerment for individuals.[36] Yet, due to the complexity of modern data processing, relying on individual choice and the use of privacy-enhancing tools is an unrealistic approach to protecting privacy, at least on a societal scale. The increased adoption of PETs at the provider-side is, on its face, an important development for reducing privacy intrusions within infrastructures that individuals cannot control.[37] It is recalled, however, that modern PETs tend to require enormous resources and accordingly tend to be embedded in the computational infrastructure controlled by the most powerful actors. Accordingly, a small set of companies control the infrastructures required for modern PETs.[38]

Among the small cohort of companies with this type of power are, of course, Google and Apple. Experience with these giants, with two examples discussed above, suggests that their conceptions of privacy may not be sufficiently expansive and human rights-informed. If privacy is conceived in a limited technical sense without appropriate consideration for the broader context, PETs actually have the potential to undermine privacy. Unfortunately, the 'Privacy' in Privacy-Enhancing Technologies tends not to account for the multifaceted and value-laden nature of the concept.[39] The design-based approach to privacy is practically limited by the technical constraints of specifications and semantics, and these systems, and the standards that support them, tend to be driven by the technology development culture.

It is important that we retain cognisance of the underlying values of privacy, including vital principles like non-domination and autonomy when assessing different privacy-enhancing solutions. Some of the issues with PETs highlight shortcomings in narrow conceptions of privacy and data protection that are solely compliance driven. If the view is adopted 'that privacy rights are coextensive with the set of explicit privacy laws and doctrines enumerated by legal rule-makers' without a fulsome consideration of privacy as a human right and societal value, gaps in protection will arise.[40] The focus of the law on atomised privacy harms, and its reliance on concepts like 'personal data' and individual data subject rights, is part of the issue with a compliance-oriented approach. Where data is analysed 'on the basis of patterns and group profiles' and is used to determine policy at a societal scale, the individual is no longer central. Decisions made based on big data analytics may not always result in an identifiable individual intrusion as traditionally conceived, but 'may still result in decisions that pose real risks on the aggregate level, for groups of, or rather grouped people.'[41] This highlights the limitations of frameworks and technologies that adopt a narrow conception of individual privacy and, as a result, overlook power imbalances and the broader collective implications of data use, leaving significant privacy harms unaddressed.

These concerns are also relevant in light of calls to clarify the concept of 'personal data', including in the European Commission's Digital Omnibus proposal for an entity-relative definition in the context of pseudonymised data.[42] The Digital Omnibus also envisions granting the power to the Commission to adopt implementing acts to specify 'means and criteria to determine whether data resulting from pseudonymisation no longer constitutes personal data for certain entities'.[43] While these suggested amendments are designed to increase legal certainty, an entity-relative interpretation risks further entrenching gaps in protection for the collective privacy harms identified in this report.[44] While these proposals seem primed to encourage increased application of privacy-enhancing techniques of pseudonymisation, the move towards a relative definition risks incentivising the use of these tools to avoid the consideration of rights.

5 Conclusion

PETs have been described as a 'technical approach to a social problem' but it is clear that technological solutionism cannot provide the full answer when privacy is a multifaceted concept of constitutive value in democratic society.[45] While privacy by design through PETs may promise to bridge the gap between law and technology, the technical approach can sometimes draw legitimacy through law while obstructing traditional legal protections.[46] Proposed reforms in the Digital Omnibus may lend further legitimacy to such practices by 'simplifying' the concept of personal data in a way that facilitates large-scale tracking and profiling and by endorsing technical solutions that tend to favour large, platform centric systems.[47]

That said, it cannot be ignored that the internal operation of technical systems is a consistent source of privacy intrusions and as a result, it remains necessary to deal with privacy issues at the technology level.[48] Through the examination of the Apple and Google case studies, this report has illustrated how the narrow focus of conventional threat models in PET design and evaluation can inadvertently compromise the protection of privacy. This highlights the urgent need for collaboration across a broad range of disciplinary expertise to address the comprehension gap between lawyers, technologists, and policymakers in order to defragment ongoing efforts to develop and deploy PETs.[49]

[*] Maria Helen Murphy (maria.murphy@mu.ie) is an Associate Professor at the Maynooth University School of Law) and Kris Shrishak (kris.shrishak@iccl.ie) is an Enforce Senior Fellow at the Irish Council for Civil Liberties. Research informing this report was presented at the

BILETA 2024 annual conference as ‘Considering the ‘Privacy’ in Privacy-Enhancing Technologies: A Dual-Disciplinary Perspective’.

[1] Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus) COM/2025/837

[2] Rónán Kennedy and Maria Helen Murphy, *Information and Communications Technology Law in Ireland* (Clarus 2017) 99; Nadezhda Purtova, ‘Private Law Solutions in European Data Protection: Relationship to Privacy, and Waiver of Data Protection Rights’ (2010) 28(2) Netherlands Quarterly of Human Rights 179; Maurizio Borghi, Federico Ferretti, and Stavroula Karapapa, ‘Online Data Processing Consent under EU Law: a Theoretical Framework and Empirical Evidence from the UK’ (2013) 21(2) International Journal of Law and Information Technology 109, 113-114; Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2016) 3; Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (Wolters Kluwer 2020) 87; Michael Rustad and Thomas Koenig, ‘Towards a Global Data Privacy Standard’ 71 Florida Law Review 365, 388; Paul Schwartz, ‘Global Data Privacy: The EU Way’ (2019) 94 New York University Law Review 771, 775; Graham Greenleaf, ‘Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories’ (2014) 23 Journal of Law, Information and Science 4.

[3] David Lyon, Surveillance Society: Monitoring Everyday Life (McGraw-Hill 2001); William Bogard, The Simulation of Surveillance: Hypercontrol in Telematic Societies (Cambridge University Press 1996); Simson Garfinkel, Database Nation (O’Reilly Media 2001).

[4] Felix Stalder, ‘The Failure of Privacy Enhancing Technologies (PETs) and the Voiding of Privacy’ (2002) 7 Sociological Research Online 25.

[5] Thijmen van Gend, ‘Privacy: The More, the Merrier?: A Case Study of How Amazon Uses Privacy Protection to Expand Its Power over IoT Manufacturers’ 9 https://repository.tudelft.nl/islandora/object/uuid%3Adb3c8752-12d2-41d8-84de-51c3cd3332c8; ‘Privacy is big business: How Big Tech instrumentalizes PETs to expand its infrastructural power’ Panel discussion with Seda Gürses, Thijmen van Gend, Donald Bertulfo, Carmela Troncoso, and Kris Shrishak (Privacy Camp 24, Brussels, 24 January 2024); Kris Shrishak, ‘PETs: Promise, expectation, hope, and reality,’ 18th International Workshop on Security (Yokohama, Japan, 30 August 2023).

[6] Woodrow Hartzog, Evan Selinger and Johanna Gunawan, ‘Privacy Nicks: How the Law Normalizes Surveillance’ (2024) 101 Washington University Law Review 717, 34.

[7] Patricia Norberg, Daniel Horne and David Horne, ‘The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors’ (2007) 41 Journal of Consumer Affairs 100; Susan Barnes, ‘A Privacy Paradox: Social Networking in the United States’ (2006) 11 First Monday; Nesrine Kaaniche, Maryline Laurent and Sana Belguith, ‘Privacy Enhancing Technologies for Solving the Privacy-Personalization Paradox: Taxonomy and Survey’ (2020) 171 Journal of Network and Computer Applications 102.

[8] Nitin Agrawal and others, ‘Exploring Design and Governance Challenges in the Development of Privacy-Preserving Computation’, *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (2021) 2.

[9] Agrawal and others (n 8).

[10] David W Archer and others, ‘UN Handbook on Privacy-Preserving Computation Techniques’ (arXiv, 15 January 2023).

[11] Michael Veale, 'Confidentiality Washing in Online Advertising' in Corinne Cath (ed), *Eaten by the Internet* (Meatspace Press 2023) 44.

[12] Information Commissioner's Office, 'Chapter 5: Privacy-Enhancing Technologies (PETs) Draft Anonymisation, Pseudonymisation and Privacy Enhancing Technologies Guidance' (Information Commissioner's Office 2022) 2–3 https://ico.org.uk/media/about-the-ico/consultations/4021464/chapter-5-anonymisation-pets.pdf; AEPD, 'Data Spaces, Sovereignty and Privacy by Design' (AEPD 28 September 2023) https://www.aepd.es/en/prensa-y-comunicacion/blog/data-spaces-sovereignty-and-privacy-by-design; Office of the Privacy Commissioner of Canada, 'Privacy Enhancing Technologies – A Review of Tools and Techniques' (OPC 15 November 2017) https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711; Office of the Privacy Commissioner of Canada, 'Privacy Tech-Know Blog: Privacy Enhancing Technologies for Businesses' (OPC 12 April 2021) https://www.priv.gc.ca/en/blog/20210412; EDPS, 'Preliminary Opinion on Privacy by Design' (European Data Protection Supervisor 2018) Opinion 5/2018 21 https://www.edps.europa.eu/sites/default/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf.

[13] EDPS, 'Preliminary Opinion on Privacy by Design' (European Data Protection Supervisor 2018) Opinion 5/2018 21 <https://www.edps.europa.eu/sites/default/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf>.

[14] European Union Agency for Cybersecurity, 'Data Protection Engineering: From Theory to Practice.' (Publications Office 2022) 9 https://data.europa.eu/doi/10.2824/09079.

[15] *Huvig v France* (1990) 12 EHRR 528; *Copland v The United Kingdom* (2007) 45 EHRR 37; *Khan v The United Kingdom* (2000) 31 EHRR 45; *Uzun v Germany* (2011) 53 EHRR 24; *Weber and Saravia v Germany* [2006] ECHR 1173; Kennedy and Murphy (n 2) 139. See also, discussion in Maria Helen Murphy, 'Privacy, Surveillance, and Democratic Values: The Adaptability of Human Rights Law in the Digital Age' in David Mangan, Gijs van Dijck, and Angela Daly (eds), The Philosophical Foundations of Information Technology Law (forthcoming).

[16] *Peck v The United Kingdom* (2003) 36 EHRR 41. The ECtHR draws on Convention No 108 in its approach. See also *Amann v Switzerland* (2000) 30 EHRR 843, paras 65-67; *Uzun v Germany* (2011) 53 EHRR 24, para 45; *S and Marper v The United Kingdom* [2008] ECHR 1581. Richard A Posner, 'The Economics of Privacy' (1981) 71 The American Economic Review 405, 405; Thomas Nagel, 'Concealment and Exposure' (1998) 27 Philosophy & Public Affairs 3.

[17] David Phillips, 'Privacy Policy and PETs: The Influence of Policy Regimes on the Development and Social Implications of Privacy Enhancing Technologies' (2004) 6 New Media & Society 691, 692; Joel R Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules through Technology' (1998) 76 Texas Law Review 553; Lawrence Lessig, *Code* (Basic Books 2006); Niels Van Dijk and others, 'Right Engineering? The Redesign of Privacy and Personal Data Protection' (2018) 32 International Review of Law, Computers & Technology 230, 11.

[18] Agrawal and others (n 8) 2; Bailey Kacsmar and others, 'Comprehension from chaos: Towards informed consent for private computation', *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security* (pp. 210-224).

[19] Yehuda Lindell, Composition of Secure Multi-Party Protocols: A Comprehensive Study (Springer 2003).

[20] Agrawal and others (n 8).

[21] Agrawal and others (n 8).

[22] Kaspar Rosager Ludvigsen, Shishir Nagaraja and Angela Daly, 'YASM (Yet Another Surveillance Mechanism)' (arXiv, 29 May 2022) 4.

[23] Lukas Struppek and others, 'Learning to Break Deep Perceptual Hashing: The Use Case NeuralHash', *2022 ACM Conference on Fairness, Accountability, and Transparency* (2022); Anunay Kulshrestha and Jonathan Mayer, 'Identifying Harmful Media in {End-to-End} Encrypted Communication: Efficient Private Membership Computation' (2021) https://www.usenix.org/conference/usenixsecurity21/presentation/kulshrestha; Ludvigsen, Nagaraja and Daly (n 22) 4.

[24] Brian Barrett, 'Apple Backs Down on Its Controversial Photo-Scanning Plans' (*Wired*, 3 September 2021) https://www.wired.com/story/apple-icloud-photo-scan-csam-pause-backlash/.

[25] Lily Hay Newman, 'Apple Kills Its Plan to Scan Your Photos for CSAM. Here's What's Next' (*Wired*, 7 December 2022) https://www.wired.com/story/apple-photo-scanning-csam-communication-safety-messages/.

[26] Lily Hay Newman, 'Apple's Decision to Kill Its CSAM Photo-Scanning Tool Sparks Fresh Controversy' (*Wired*, 31 August 2023) https://www.wired.com/story/apple-csam-scanning-heat-initiative-letter.

[27] While the EU failed to pass legislation requiring mandatory scanning, a compromise position has been reached by the Council that would require online service providers to adopt proportionate technical and organisational measures to mitigate child sexual abuse and make permanent provision for the voluntary scanning of services for child sexual abuse. Council of the EU, 'Child sexual abuse: Council reaches position on law protecting children from online abuse' (Press Release, 26 November 2025) https://data.consilium.europa.eu/doc/document/ST-15318-2025-INIT/en/pdf.

[28] Anthony Chavez, 'Update on Plans for Privacy Sandbox Technologies' (*Privacy Sandbox*, 17 October 2025) https://privacysandbox.google.com/blog/update-on-plans-for-privacy-sandbox-technologies; Anthony Chavez, 'Next Steps for Privacy Sandbox and Tracking Protections in Chrome' (*Privacy Sandbox*, 22 April 2025) https://privacysandbox.com/news/privacy-sandbox-next-steps; Anthony Chavez, 'A New Path for Privacy Sandbox on the Web' (*Privacy Sandbox*, 22 July 2024) https://privacysandbox.com/news/privacy-sandbox-update.

[29] Yohan Beugin and Patrick McDaniel, 'Interest-Disclosing Mechanisms for Advertising Are Privacy-Exposing (Not Preserving)' (2024) *Proceedings of Privacy Enhancing Technologies* 41; Peter Snyder, 'Google's Topics API: Rebranding FLoC Without Addressing Key Privacy Issues' (Brave, 25 January 2022) https://brave.com/web-standards-at-brave/7-googles-topics-api/.

[30] Beugin and McDaniel (n 29) 41–45; van Gend (n 5) 9; 'Privacy is big business: How Big Tech instrumentalizes PETs to expand its infrastructural power' (n 5); Emiliano De Cristofaro and others (2025), 'PETs and AI: Privacy Washing and the Need for a PETs Evaluation Framework (Dagstuhl Seminar 25112)', *Dagstuhl Reports*, *15*(3), 77-93.

[31] Competition and Markets Authority, 'Investigation into Google's "Privacy Sandbox" Browser Changes' https://www.gov.uk/cma-cases/investigation-into-googles-privacy-sandbox-browser-changes.

[32] Michael Veale and Frederik Zuiderveen Borgesius, 'Adtech and Real-Time Bidding under European Data Protection Law' (2022) 23 German Law Journal 226.

[33] For related discussion in the context of traditional PETs see Stalder (n 4) 9.

[34] Neil Richards, *Why Privacy Matters* (Oxford University Press 2021) 50; Hartzog, Selinger and Gunawan (n 6) 56.

[35] Agrawal and others (n 8)10.

[36] Stalder (n 4).

[37] Agrawal and others (n 8) 4.

[38] Veale (n 11) 45; Thijmen van Gend, Donald Jay Bertulfo, and Seda Gürses. 'The PET Paradox'.

[39] Seda Gürses and Bettina Berendt, 'PETs in the Surveillance Society: A Critical Review of the Potentials and Limitations of the Privacy as Confidentiality Paradigm' in Serge Gutwirth, Yves Poullet and Paul De Hert (eds), *Data Protection in a Profiled World* (Springer Netherlands 2010); Phillips (n 17); Stalder (n 4); Herman T Tavani and James H Moor, 'Privacy Protection, Control of Information, and Privacy-Enhancing Technologies' (2001) 31 Computers and Society 6.

[40] Harry Surden, 'Structural Rights in Privacy' (2007) 60(4) Southern Methodist University 1605, 1607; Hartzog, Selinger and Gunawan (n 6) 13.

[41] Linnet Taylor, 'Safety in Numbers? Group Privacy and Big Data Analytics in the Developing World' in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy: New Challenges of Data Technologies* (Springer International Publishing 2017). Rainer Mühlhoff and Hannah Ruschemeier, 'Predictive Analytics and the Collective Dimensions of Data Protection' (2024) 16 Law, Innovation and Technology 261.

[42] Digital Omnibus, art 3(1).

[43] Digital Omnibus, art 3(10).

[44] And is related to recent case law *European Data Protection Supervisor v Single Resolution Board* (C-413/23 P) EU:C:2025:645. See also *Patrick Breyer v Bundesrepublik Deutschland* (C-582/14) EU:C:2016:779.

[45] George Danezis and others, *Privacy and Data Protection by Design - from Policy to Engineering* (ENISA 2014) 48; Seda Gürses, 'Can You Engineer Privacy?' (2014) 57 Communications of the ACM 20.

[46] Tavani and Moor (n 39) 25.

[47] 'The EU's Digital Omnibus offers relief for ad tech, but hands more power to Big Tech and AI agents' (Digiday, 21 November 2025) https://digiday.com/marketing/the-eus-digital-omnibus-offers-relief-for-ad-tech-but-hands-more-power-to-big-tech-and-ai-agents.

[48] Danezis and others (n 45) 48.

[49] Agrawal and others (n 8) 6.