Routledge
Taylor & Francis Group

Information & Communications Technology Law

ISSN: 1360-0834 (Print) 1469-8404 (Online) Journal homepage: https://www.tandfonline.com/loi/cict20

Technological solutions to privacy questions: what is the role of law?

Maria Helen Murphy

To cite this article: Maria Helen Murphy (2016) Technological solutions to privacy questions: what is the role of law?, Information & Communications Technology Law, 25:1, 4-31, DOI: 10.1080/13600834.2015.1134148

To link to this article: https://doi.org/10.1080/13600834.2015.1134148

Information & Communications Technology Law, 2016
Vol. 25, No. 1, 4–31, http://dx.doi.org/10.1080/13600834.2015.1134148

Routledge
Taylor & Francis Group

Technological solutions to privacy questions: what is the role of law?

Maria Helen Murphy*

Law Department, Maynooth University, Co. Kildare, Ireland

In spite of its recognition as a fundamental human right, privacy is sometimes criticised as an anachronistic value in modern life [James Rule, *Privacy in Peril* (OUP, 2007) xi]. While the prominence of this view has lessened in the wake of the Snowden revelations and increased public concern with online privacy [Maria Helen Murphy, 'The Pendulum Effect: Comparisons Between the Snowden Revelations and the Church Committee. What are the Potential Implications for Europe?' (2014) 23(2) *Information and Communications Technology Law* 192], the right continues to struggle for support when it is portrayed as being in competition with national security, personal safety, and economic prosperity [Daniel Solove, '"I've Got Nothing to Hide" and other Misunderstandings of Privacy' (2007) 44 San DLR 745]. As developments in technology continue to threaten the right to privacy, interest in technological solutions to privacy problems continues to grow. This article seeks to consider current privacy debates from the perspectives of multiple stakeholders in order to assess whether technological and design approaches offer the best path forward, or whether an essential role remains to be played by law.

Keywords: privacy by design; encryption; incentives; technology

Introduction

Privacy is widely found in international human rights instruments, but in spite of this legal recognition, privacy has been criticised as a moribund right of little value in the modern world.[1] In the post-Snowden environment, however, there has been a reinvigoration of the privacy debate.[2] Even some so-called 'digital natives' have expressed renewed interest in privacy and have, to an extent, voted with their feet, by embracing Internet services that market the privacy conscious features of their products as key selling points.[3] While increased focus on anonymity tools and encryption software appears to be a positive sign for the continued protection of privacy rights, important questions remain regarding the role law has to play in this context.[4]

*Email: maria.murphy@nuim.ie

[1]James Rule, *Privacy in Peril* (OUP, 2007) xi.

[2]Maria Helen Murphy, 'The Pendulum Effect: Comparisons between the Snowden Revelations and the Church Committee. What are the Potential Implications for Europe?' (2014) 23(2) *Information and Communications Technology Law* 192.

[3]Parmy Olson, 'Delete By Default: Why More Snapchat-Like Messaging Is On Its Way' *Forbes* (22 November 2013) <www.forbes.com/sites/parmyolson/2013/11/22/delete-by-default-why-more-snapchat-like-messaging-is-on-its-way/> accessed 27 August 2015; Chris Johnston, 'DuckDuckGo Traffic Soars in Wake of Snowden Revelations' *The Guardian* (London 17 June 2015) <www.theguardian.com/technology/2015/jun/17/duckduckgo-traffic-snowden-revelations> accessed 27 August 2015.

The Snowden revelations clarified and confirmed the vast capabilities of modern intelligence agencies. As technology improves – and as individual engagement with communications technology increases – it is almost trite to state that privacy protecting laws often lag behind technological developments.[5] Technological solutions to privacy problems, however, can be much more responsive to new and evolving threats to privacy. Many in the technology community have adopted the development of privacy protecting solutions as a mission and have designed tools that protect against personal, corporate, and government surveillance. Equally, however, governments seek to counter such tools of opacity by both exploiting technological weaknesses and exploring legal options in an effort to hinder their continued development. This article examines the challenges to privacy that exist in the modern world and considers what role legislative tools have to play in the protection of privacy in this red queen's race. In order to illustrate how technological solutions can further the protection of privacy, this article considers the potential of adopting a 'privacy by design' approach in the context of unmanned aerial vehicles (UAVs, commonly known as 'drones'). Building from this analysis, this article assesses the role encryption can play in the protection of online communications. Crucially, even though encryption is a technological tool used to protect privacy, this article considers the role that law and legal rights can play in the restriction and use of such tools. An important aspect of the approach adopted in this article is the continued focus on the knowable incentives of the various stakeholders. The author maintains that cognisance of such motivations is essential if effective solutions are to be identified.

Different interests

It is clear that the protection of privacy involves many interests. The manner in which privacy protections are implemented has implications for numerous actors with sometimes overlapping

[4]It is not unusual for government to seek alternative means to regulate behaviour in addition or in place of legislative action. For example, a government can make undesirable conduct more difficult or impossible through 'architecture' modifications. A simple example of this is when a government installs speed bumps in order to deter speeding. Ryan Calo, 'Code, Nudge, or Notice' (2014) 99 Iowa L Rev 773, 778. Architectural solutions have particular benefits in the context of the Internet as famously articulated by Lawrence Lessig. According to Lessig's major text on this issue 'The software and hardware that make cyberspace what it is constitute a set of constraints on how you can behave. The substance of these constraints may vary, but they are experienced as conditions on your access to cyberspace.' According to Lessig

> [t]he code or software or architecture or protocols set these features; they are features selected by code writers; they constrain some behavior by making other behavior possible, or impossible. … In this sense, it too is regulation, just as the architectures of real-space codes are regulations.

Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books, 1999) 89. See also, Lawrence Lessig, *Code: Version 2.0* (Basic Books, 2006); Joel Reidenberg has argued that code is a 'useful extra-legal instrument that may be used to achieve objectives that otherwise challenge conventional laws'. Joel Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules Through Technology' (1998) 76 Tex L Rev 553, 556.

[5]Daniel Solove, *Understanding Privacy* (Harvard University Press, 2008) 62–63; Mark O' Brien, 'Law, Privacy, and Information Technology: A Sleepwalk through the Surveillance Society?' (2008) 17 ICTL 25, 28.

– and sometimes diverging – motivations. This article highlights four key stakeholders that must be considered when evaluating policy choices in this area: the individual/consumer, the government and its' agencies, technology companies, and security professionals. It is important to recognise the multiplicity of interests that influence each of these actors.

The individual/consumer, for example, has several interests at issue. For one, the individual/consumer wishes to enjoy the consumer goods produced by technology companies. The effectiveness of Internet services – such as Google Now – may, at times, require the collection of large amounts of personal data.[6] It could be argued that a better consumer experience is provided where this information is collected seamlessly and with minimal interruption or involvement of the consumer. In spite of this incentive to share data with technology companies, the individual/consumer also has an interest in the protection of privacy from both an individual and a societal perspective.[7] In addition, many individuals/consumers will identify an interest in government surveillance where such surveillance assists in crime control and national security. Accordingly, we can readily identify three distinct interests that have the potential to influence the attitude and approach of the average individual to privacy protection.

Technology companies are another key actor and they have clear economic incentives to collect large amounts of data.[8] Online services are also incentivised to store data unencrypted as it is much easier to monetise than unreadable data.[9] In addition to this motivation, technology companies are incentivised to keep both governments and customers happy. With the ongoing migration of communications to the Internet and the Cloud, technology companies have become a 'key component of the surveillance infrastructure'.[10] As governments have a surveillance interest in accessing stored data, technology companies may be encouraged to increase their collection and retention of personal information. Of course, as some Internet services operate more effectively with large data sets, increasing the collection and retention may also provide the company with some competitive advantage. Equally, however, where a company is facing back-lash from privacy conscious users they will be incentivised to build in additional privacy protections and to minimise certain types of data collection.[11]

The primary goal of a security engineer is to ensure the relevant system is 'dependable in the face of malice, error, or mischance'.[12] As adequate information security is a condition precedent for privacy, the work of security engineers has significant benefits for the

[6]Simon Hill, 'How to get the Best out of Google Now' *Digital Trends* (11 June 2015) <www.digitaltrends.com/users/simonhill/> accessed 27 August 2015.

[7]Privacy plays an essential role in liberal democratic society. Alan Westin, *Privacy and Freedom* (Atheneum, 1967) 24.

[8]Perry Rotella, 'Is Data The New Oil?' *Forbes* (2 April 2012) <www.forbes.com/sites/perryrotella/2012/04/02/is-data-the-new-oil/> accessed 27 August 2015.

[9]For example, if data stored on a service is encrypted and the service provider is not privy to the key, the company will be unable to analyse that data in order to display targeted advertising. Christopher Soghoian, 'Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era' (2010) 8 J Telecomm & High Tech L 359, 395.

[10]Christopher Soghoian, 'Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era' (2010) 8 J Telecomm & High Tech L 359, 395, 386.

[11]Fatemeh Khatibloo and others, 'When Customers Take Control' (Forrester, July 2015) <https://www.forrester.com/Brief+When+Customers+Take+Control/fulltext/-/E-res121723> accessed 27 August 2015.

[12]Ross Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems* (Wiley, 2010) 3.

protection of privacy. While secure systems help protect the privacy rights that are important for individuals, secure systems also provide significant economic and societal benefits that both technology companies and governments value.[13] The other side to this, of course, is that secure systems can pose a challenge to governments with an interest in surveillance. This throws the conflict between these competing goals into sharp relief.

Appreciation of these overlapping and diverging interests is important as it provides the context necessary to address the question of how we may choose to regulate this area. It is clear that these relationships are complex and should not be reduced to general assumptions. This point is illustrated well by the nuanced relationship between the citizen and the state in this area. While the interests of the individual/consumer and his or her government may seem to be diametrically opposed when viewed from a privacy and surveillance perspective, the protection of Internet and national security results in some overlap between the interests of both parties. As additional overlapping interests can be identified, it is important to focus and foster common interests. Such an approach has the potential to be more effective than solely relying on legal means of control.

Privacy by design

A well-established example of a more technological- or design-based approach to privacy protection is the 'privacy by design' approach. While 'privacy by design' is a well-established concept, it is important to consider the definition of the term in order to orient the discussion.[14] The principle of privacy by design has been described as a 'systematic approach to designing any technology that embeds privacy into the underlying specifications or architecture'.[15] While a privacy by design approach is frequently described as constituting best practice, the approach has also been increasingly mandated as an essential aspect of data protection law compliance. For example, the proposed European Union Data Protection Regulation requires the adoption of data protection by design and by default.[16]

[13]European Commission, 'Cybersecurity' (European Commission Digital Agenda for Europe, 2 March 2015) <https://ec.europa.eu/digital-agenda/en/cybersecurity> accessed 27 August 2015.

[14]It is interesting to note that while the concept of privacy by design originated from the Office of the Information and Privacy Commissioner of Ontario, the principle has subsequently been recognised as 'an essential component of fundamental privacy protection' globally. Ann Cavoukian, *Privacy by Design* (Information and Privacy Commissioner 2009) 1 <https://www.ipc.on.ca/images/resources/privacybydesign.pdf> accessed 27 August 2015.

[15]Ira Rubinstein, 'Regulating Privacy by Design' (2011) 26 Berkeley Tech LJ 1410, 1411–1412; Ann Cavoukian, *Privacy by Design* (Information and Privacy Commissioner 2009) 1 <https://www.ipc.on.ca/images/resources/privacybydesign.pdf> accessed 27 August 2015; Maria Helen Murphy, 'The Introduction of Smart Meters in Ireland: Privacy Implications and the Role of Privacy by Design' (2015) 38(1) *Dublin University Law Journal*.

[16]It is important to note that the draft Regulation does not provide additional details as to what 'privacy by design' entails or what types of technical solutions such an approach requires. Bert-Jaap Koops and Ronald Leenes, 'Privacy Regulation Cannot be Hardcoded. A Critical Comment on the "Privacy By Design" Provision in Data-Protection Law' (2014) 28 IRLCT 159, 160. Commission (EC), 'Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation)' COM (2012) 11 final. Regardless of potential reforms, it has been argued that a privacy by design requirement is already implied by Article 17 of the Data Protection Directive. Ian Brown, 'Britain's Smart Meter Programme: A Case Study in Privacy by Design' (2014) 28 IRLCT 172, 176; Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data [1995] OJ L281/31.

For the purposes of this article, one of the most relevant tenets of the privacy by design approach is that privacy by design should be applied in a 'positive-sum' manner where possible. Instead of relying on trade-offs between privacy and other interests, a privacy by design approach seeks a solution that best reconciles the different aims.[17] As it has been put by Privacy by Design's most noted advocate, Ann Cavoukian:

> Privacy can and must co-exist alongside other critical requirements: security, functionality, operational efficiency, organizational control, business processes, and usability in a 'positive-sum', or doubly enabling 'win-win' equation. How we get there is through Privacy by Design.[18]

This approach aims to incentivise the protection of privacy by rejecting the 'zero-sum paradigm' that characterises privacy as an 'impediment standing in the way of innovation and desired goals'.[19] It has been shown that many of the features of a privacy by design approach – such as data minimisation and data security – will not impair the legitimate goals of innovation where privacy is considered from the initial design stages.[20]

UAVs and privacy by design

A key aspect of the privacy by design approach calls for the privacy implications of new systems and technologies to be considered from the outset.[21] Such early consideration avoids costly retrofitting and facilitates the adoption of privacy maximising solutions that do not interfere with the core purpose of a new system or technology.[22] The principles of privacy by design have broad potential applicability. For example, it has been argued that technology companies – including Google and Facebook – would have avoided privacy scandals and loss of consumer confidence without negatively affecting their performance if the companies had adopted a privacy by design approach.[23] It is also contended that the adoption of privacy by design when designing large infrastructural programmes has the potential to save governments significant resources and avoid public relations

[17]Ann Cavoukian, 'Privacy and Radical Pragmatism: Change the Paradigm' (Information and Privacy Commissioner 2008) 16 <http://www.ipc.on.ca/images/Resources/radicalpragmatism_1.pdf> accessed 27 August 2015.
[18]Ann Cavoukian, 'Privacy by Design: The Definitive Workshop, a Foreword' (2010) 3 *Identity in the Information Society* 247–51, 248.
[19]Ann Cavoukian, 'Privacy and Radical Pragmatism: Change the Paradigm' (Information and Privacy Commissioner 2008) 16 <http://www.ipc.on.ca/images/Resources/radicalpragmatism_1.pdf> accessed 27 August 2015; Maria Helen Murphy, 'The Introduction of Smart Meters in Ireland: Privacy Implications and the Role of Privacy by Design' (2015) 38(1) *Dublin University Law Journal*.
[20]Ann Cavoukian, 'Privacy and Radical Pragmatism: Change the Paradigm' (Information and Privacy Commissioner 2008) 16 <http://www.ipc.on.ca/images/Resources/radicalpragmatism_1.pdf> accessed 27 August 2015; Maria Helen Murphy, 'The Introduction of Smart Meters in Ireland: Privacy Implications and the Role of Privacy by Design' (2015) 38(1) *Dublin University Law Journal*.
[21]Ann Cavoukian, *Privacy by Design* (Information and Privacy Commissioner 2009) 1 <https://www.ipc.on.ca/images/resources/privacybydesign.pdf> accessed 27 August 2015.
[22]Ian Brown, 'Britain's Smart Meter Programme: A Case Study in Privacy by Design' (2014) 28 IRLCT 172, 176; Maria Helen Murphy, 'The Introduction of Smart Meters in Ireland: Privacy Implications and the Role of Privacy by Design' (2015) 38(1) *Dublin University Law Journal*.
[23]Ira Rubinstein and Nathan Good, 'Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents' (2013) 28 Berkeley Tech LJ 1333.

problems.[24] The recent popularisation of UAV technology provides a useful and timely example to illustrate the merits of a privacy by design approach.[25]

With the increased sophistication and proliferation of UAV technology, there are growing regulatory and privacy challenges surrounding the use of UAVs. From the basic regulatory angle, there are safety and security concerns.[26] In addition to these issues, the increased adoption of UAVs also raises clear privacy questions.[27] In the past, UAVs have been used primarily as a military technology, but due to the reduction in price and increased accessibility of such technologies, the recreational user is growing in significance.[28]

The use of recreational UAVs has been a popular topic of debate in recent years, and the technology attracted significant news coverage in 2015 when a UAV landed on White House property.[29] While this was an accidental landing, the incident highlighted the security risk created by the technology. One interesting outcome of the scandal was the imposition of a 'no drone zone' over Washington, DC, by the market-leading UAV manufacturer, DJI.[30] DJI upgraded their firmware geo-fencing software in order to prevent Phantom UAVs from flying over the Washington, DC, area in the future.[31] This decision supports the existing Federal Aviation Administration rules that deem Washington, DC, airspace to be a flight restricted zone.[32] The geo-fencing restrictions imposed by DJI on its customers could be seen as a service enhancement that prevents an informed customer from unwittingly breaking the law.

[24]Ian Brown, 'Britain's Smart Meter Programme: A Case Study in Privacy by Design' (2014) 28 IRLCT 172, 176; Maria Helen Murphy, 'The Introduction of Smart Meters in Ireland: Privacy Implications and the Role of Privacy by Design' (2015) 38(1) *Dublin University Law Journal*.

[25]Article 29 Data Protection Working Party, 'Opinion 01/2015 on Privacy and Data Protection Issues Relating to the Utilisation of Drones' (Adopted on 16 June 2015) <ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf> accessed 27 August 2015.

[26]Roger Clarke and Lyria Bennett Moses, 'The Regulation of Civilian Drones: Impacts on Public Safety' (2014) 30 CLSR 263.

[27]Benjamin Kapnik, 'Unmanned But Accelerating: Navigating The Regulatory and Privacy Challenges of Introducing Unmanned Aircraft into the National Airspace System' (2012) 77 J Air L & Com 439.

[28]Kevin Poulsen, 'Why the US Government Is Terrified of Hobbyist Drones' *Wired* (5 February 2015) <www.wired.com/brandlab/2015/02/white-house-drone/> accessed 27 August 2015; Clay Dillow, 'Get Ready for "Drone Nation"' *Fortune* (8 October 2014) <fortune.com/2014/10/08/drone-nation-air-droid/> accessed 27 August 2015.

[29]Jim Acosta and Jeremy Diamond, 'US Intel Worker Blamed for White House Drone Crash' *CNN* (27 January 2015) <edition.cnn.com/2015/01/26/politics/white-house-device-secret-service/index.html?iid=EL> accessed 27 August 2015; For a similar case see Michael Schmidt, 'Secret Service Arrests Man After Drone Flies Near White House' *New York Times* (New York 14 May 2015) <www.nytimes.com/2015/05/15/us/white-house-drone-secret-service.html> accessed 27 August 2015.

[30]Ben Bjostad, 'DJI Announces No-Fly-Zone Expansion Over Washington DC' *UAV Experts* (28 January 2015) <www.uavexpertnews.com/dji-announces-no-fly-zone-expansion-over-washington-d-c/> accessed 27 August 2015.

[31]Ben Bjostad, 'DJI Announces No-Fly-Zone Expansion Over Washington DC' *UAV Experts* (28 January 2015) <www.uavexpertnews.com/dji-announces-no-fly-zone-expansion-over-washington-d-c/> accessed 27 August 2015.

[32]Jose Pagliery, 'No, You Can't Fly Drones Over The White House' *CNN* (26 January 2015) <money.cnn.com/2015/01/26/technology/security/drone-white-house/> accessed 27 August 2015.

The privacy risk posed by UAVs is heightened by low barriers-to-entry to UAV ownership and the affordability of video recording technology.[33] The risk is further compounded by the difficulties of enforcement and education in the fields of data protection and privacy. In light of these challenges, the technological solution chosen by DJI to counter the physical security risk posed by such devices could also be applied to address the privacy risk.

While imposing broad 'no drone zones' would clearly have benefits for privacy, such zones would be detrimental to the interests of UAV manufacturers and their customers. Accordingly, when national security is not the primary concern, it makes sense to design the technology with privacy in mind in an attempt to head off the compliance challenge without undue cost being imposed on the multiple stakeholders. One way for UAV manufacturers to incorporate privacy by design principles would be to build in 'no record zones' as opposed to 'no drone zones' into their software. The location of 'no record zones' could be determined based on residential status or else by an opt-out registration system.[34]

The advantage of such an approach is that the collection of personal data would be minimised and hobbyists would not be prevented from flying their UAVs safely and in accordance with privacy principles. Instead of simply expecting users to apply complex data protection rules to their use of such technologies, privacy intrusion could be minimised from the outset by designing privacy solutions into the products. As UAV manufacturers have a strong incentive to appear responsible in order to make the case for less onerous regulation, there are clear benefits for the industry to embrace such technological solutions. While regulation may be necessary to incentivise privacy consciousness, 'hard-coding' compliance into a product has the potential to be more effective than expecting the average hobbyist to educate themselves on their legal requirements. Considering the relatively low risk of enforcement for the average recreational user, imposing onerous regulations may in fact be more likely to encourage complete non-compliance rather than complete non-engagement with the technology.[35]

While it is likely that a determined individual will be able to bypass geo-fencing restrictions, the privacy harm created by the average hobbyist would be greatly mitigated.[36] Such an attempt to reconcile the interests of the different stakeholders has the potential to prevent

[33]Not only does drone technology erase the 'natural limits' associated with traditional aerial surveillance, but it also facilitates new forms of invasion. Jay Stanley, 'We Already Have Police Helicopters, So What's the Big Deal Over Drones?' (ACLU 8 March 2013) <https://www.aclu.org/blog/we-already-have-police-helicopters-so-whats-big-deal-over-drones?redirect=blog/technology-and-liberty-criminal-law-reform/we-already-have-police-helicopters-so-whats-big-deal> accessed 27 August 2015.

[34]To provide an example of how this might work, NoFlyZone.org is a website that allows individuals to register their address in a database in order to notify drone operators that you do not want drones flying over your property. While DJI has not signed up to this programme, several other major manufacturers and navigation platforms (including Horizon Hobby, EHANG, and HEXO+, PixiePath and RCFlyMaps) have. Lily Hay Newman, 'Here's How to Set Up a No-Fly Drone Zone Over Your House' *Slate* (10 February 2015) <www.slate.com/blogs/future_tense/2015/02/10/noflyzone_org_lets_you_geofence_the_area_over_your_house_for_drones_to_avoid.html> accessed 27 August 2015; Frederic Lardinois, 'NoFlyZone Lets You Establish A No-Fly Zone Over Your Property' *Tech Crunch* (9 February 2015) <techcrunch.com/2015/02/09/noflyzone-lets-you-establish-a-no-fly-zone-over-your-property/> accessed 27 August 2015.

[35]Tim McCarthy, 'Geospatial Platform for Safe and Regulated and Non-Intrusive UAS Operation' (Privacy: Gathering Insights from Lawyers and Technologists Conference, Maynooth University, Ireland, 1 July 2015).

[36]Some bypassing is likely to occur, even if geo-fencing restrictions are legislatively mandated. Kevin Poulsen, 'Why the US Government Is Terrified of Hobbyist Drones' *Wired* (5 February 2015) <www.wired.com/brandlab/2015/02/white-house-drone/> accessed 27 August 2015.

wide-scale flouting of data protection rules and better recognises the limitations of enforcement when a practice is widespread and difficult to detect. This 'no record zone' example illustrates how technological solutions have the potential to enhance privacy without alienating key stakeholders. With the support of product manufacturers and service providers, the effectiveness of privacy protection should increase.

Implications of design/technological solutions to privacy questions in the surveillance context

In spite of the existence of positive examples that illustrate the potential for positive sum solutions to privacy questions in the corporate context, it is clear that when considering the interests of competing and occasionally cooperating actors, different considerations come to the fore in the surveillance and national security context. The additional difficulties associated with privacy protection in the national security context are highlighted by Daniel Solove who warns against the temptation to summarily dismiss the classic 'nothing to hide, nothing to fear' argument.[37] While there are many ways to criticise the 'nothing to hide, nothing to fear' position, it is important to recognise the significant sway this position holds over many when it is applied in the national security context.[38] When considering the incentives that influence the actions of key stakeholders, it is important to recognise the influence this argument holds.

Bearing the additional challenges that arise in the national security context in mind, the following section addresses the importance of encryption technology for the protection of privacy and also considers how the various stakeholders can be incentivised to support such technology. A key aspect of this discussion considers whether governments with surveillance interests can be won over by purely technological and security focused arguments and assesses what role can be played by legal obligations.

Encryption

A clear manifestation of the struggle between privacy enhancing technologies and government surveillance is the encryption tug-of-war that has, once again, become a significant source of contention between technology companies and law enforcement/surveillance agencies. A basic definition describes encryption as a 'process of converting messages, information, or data into a form unreadable by anyone except the intended recipient'.[39]

---

[37]While the 'nothing to hide' argument's 'superficial incantations can readily be refuted', Solove points out that when 'the argument is made in its strongest form, it is far more formidable'. Daniel Solove, '"I've got Nothing to Hide" and other Misunderstandings of Privacy' (2007) 44 San DLR 745, 747, 753.

[38]Solove points out how

> [c]ast in this manner, the nothing to hide argument is a formidable one. It balances the degree to which an individual's privacy is compromised by the limited disclosure of certain information against potent national security interests. Under such a balancing scheme, it is quite difficult for privacy to prevail.

Daniel Solove, '"I've got Nothing to Hide" and other Misunderstandings of Privacy' (2007) 44 San DLR 745, 753.

[39]See SANS Institute, 'History of Encryption' (SANS Institute White Paper 2001) <http://www.sans.org/reading-room/whitepapers/vpns/history-encryption-730> accessed 27 August 2015 and Human Rights Council, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye' (2015) UN Doc A/HRC/29/3, 4.

The goal of such conversion is to protect the 'confidentiality and integrity' of content against unauthorised third-parties.[40]

Encryption can be achieved in a number of different ways. Symmetric-key encryption uses the same secret key to encrypt data that is used to decrypt data.[41] A clear challenge to such encryption is the need to securely exchange the secret key with the party you wish to communicate with.[42] As this may often require an in-person meeting, symmetric and secret key encryption is an unattractive solution in the modern world.[43] This problem was resolved to a significant extent with the advent of public key encryption, which utilises a second key.[44] The first key is public and can be shared with individuals who may wish to communicate with the owner of the public key.[45] By having access to the public key, the data can be correctly encoded by the data senders. A second, private and non-inferable, key is required to decrypt the data.[46] As the data recipient is the only individual with access to the private second key, they can decrypt the message securely.[47] Asymmetric public key encryption can also be used to transfer a symmetric secret key securely.[48] While this example explains encryption by discussing the protection of 'data in motion', encryption can also be used to protect 'data at rest'. Data at rest includes data stored on a computer hard drive, smart phone, and now data at rest can include data stored on the Cloud.[49]

Historically, sophisticated encryption and decryption was primarily practiced by competing governments seeking military or political advantage.[50] In more recent times, however, the significance of the Internet for communications and transactions has ensured the importance of encryption for the general population.[51] As pointed out by

[40]Human Rights Council, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye' (2015) UN Doc A/HRC/29/3, 4; Susan Landau, 'Under the Radar: NSA's Efforts to Secure Private-sector Telecommunications Infrastructure' (2014) 7 J Nat'l Sec L & Pol'y 411, 411, 419.

[41]John Palfrey, 'Security and the Basics of Encryption in E-Commerce' (Berkman Center for Internet and Society 2001) <http://cyber.law.harvard.edu/ecommerce/encrypt.html> accessed 27 August 2015; Hans Delfs and Helmut Knebl, *Introduction to Cryptography* (Springer, 2007) 11–31.

[42]Hans Delfs and Helmut Knebl, *Introduction to Cryptography* (Springer, 2007) 11–31.

[43]Gordon Corera, *Intercept: The Secret History of Computers and Spies* (Weidenfeld & Nicholson, 2015) 112.

[44]John Palfrey, 'Security and the Basics of Encryption in E-Commerce' (Berkman Center for Internet and Society 2001) <http://cyber.law.harvard.edu/ecommerce/encrypt.html> accessed 27 August 2015; see Whitfield Diffie and Martin Hellman, 'New Directions in Cryptography' (1976) 22 *IEEE Transactions on Information Theory* 644.

[45]Such public keys are now frequently seen on the *Twitter* pages of journalists in order to encourage sources to make contact.

[46]It is non-inferable by reason of the complexity of inverting the encryption method; knowing the public key does not benefit decryption efforts. Susan Landau, 'Under the Radar: NSA's Efforts to Secure Private-sector Telecommunications Infrastructure' (2014) 7 J Nat'l Sec L & Pol'y 411, 411, 419.

[47]John Palfrey, 'Security and the Basics of Encryption in E-Commerce' (Berkman Center for Internet and Society 2001) <http://cyber.law.harvard.edu/ecommerce/encrypt.html> accessed 27 August 2015.

[48]Hans Delfs and Helmut Knebl, *Introduction to Cryptography* (Springer, 2007) 11–31.

[49]Frank Ohlhorst, 'Encryption is Front-Line Defense for Data at Rest' *Tech Republic* (3 July 2014) <www.techrepublic.com/article/encryption-is-front-line-defense-for-data-at-rest/> accessed 27 August 2015.

[50]Gordon Corera, *Intercept: The Secret History of Computers and Spies* (Weidenfeld & Nicholson, 2015) 104–105.

[51]Gordon Corera, *Intercept: The Secret History of Computers and Spies* (Weidenfeld & Nicholson, 2015) 104–105.

Sarah McKune, anonymity and encryption tools 'impact the digital security of the vast majority of the public' by protecting the financial data of consumers and by defending against 'politically motivated digital attacks'.[52] In spite of the many benefits of encryption, some view the practice as inherently suspicious when utilised by members of the public.[53]

As governments world-wide have, once again, begun to speak up in opposition to encryption technology,[54] some commentators suggest that we are currently in the midst of 'Crypto Wars II'.[55] Accordingly, it is logical to consider whether any lessons can be gleaned from the original Crypto Wars debate. The background to 'Crypto-Wars I' is provided by the decision of the US government to place strong encryption systems on the Munitions List.[56] In order to export a technology that has been placed on the Munitions List, an export licence must be obtained from the State Department.[57] While exclusive access to advanced encryption technology has clear value to government powers, significant problems with this export focused approach began to emerge in the 1970s when private industry had started to develop advanced cryptographic solutions in anticipation of increased computer use in consumer transactions and communications.[58]

The issue became unavoidable in the 1990s when Internet transactions and mobile communications were widely commercialised.[59] Phil Zimmermann – the creator of the popular email encryption software, Pretty Good Privacy – was under criminal investigation for three years as a result of the export restrictions.[60] Although exports controls only restricted products that were to be sent abroad, production costs and design considerations meant that many technology companies 'eschewed the use of strong cryptography' in products intended for both foreign and domestic markets.[61] As Schneier points out, doing so was

[52]Sarah McKune, 'Encryption, Anonymity, and the "Right to Science"' *Just Security* (28 April 2015) <justsecurity.org/22505/encryption-anonymity-debates-right-science/> accessed 27 August 2015.
[53]Jeffrey Vagle, 'Furtive Encryption: Power, Trust, and the Constitutional Cost of Collective Surveillance' (2015) 90 Indiana LJ 101, 104–105.
[54]Of course, in spite of challenges, several governments support encryption. For example, Brazil and Austria both have laws that protect the use of encryption by individuals. Marco Civil da Internet Law of Brazil 2014; E-Commerce Act and Telecommunication Act of Austria 2001; Human Rights Council, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye' (2015) UN Doc A/HRC/29/3, 13.
[55]Bruce Schneier, 'More Crypto Wars II' *Schneier on Security* (21 October 2014) <https://www.schneier.com/blog/archives/2014/10/more_crypto_war.html> accessed 27 August 2015; Sascha Meinrath and Sean Vitka, 'Crypto War II' (2014) 31 *Critical Studies in Media Communication* 123.
[56]Sharon Black, *Telecommunications Law in the Internet Age* (Morgan Kauffman, 2002) 353; US Munitions List.
[57]Sharon Black, *Telecommunications Law in the Internet Age* (Morgan Kauffman, 2002) 353; US Munitions List; Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (WW Norton & Company, 2015) 119.
[58]Susan Landau, 'Under the Radar: NSA's Efforts to Secure Private-sector Telecommunications Infrastructure' (2014) 7 J Nat'l Sec L & Pol'y 411, 411, 418.
[59]Susan Landau, 'Under the Radar: NSA's Efforts to Secure Private-sector Telecommunications Infrastructure' (2014) 7 J Nat'l Sec L & Pol'y 411, 411, 419.
[60]Announcement from Philip Zimmermann's Lead Defense Counsel (12 January 1996) <https://www.philzimmermann.com/EN/news/PRZ_case_dropped.html> accessed 27 August 2015; Gordon Corera, *Intercept: The Secret History of Computers and Spies* (Weidenfeld & Nicholson, 2015) 123–124; Steve Ranger, 'Defending the Last Missing Pixels: Phil Zimmermann Speaks Out On Encryption, Privacy, and Avoiding a Surveillance State' *Tech Republic* (23 June 2015) <www.techrepublic.com/article/defending-the-last-missing-pixels-phil-zimmermann/> accessed 27 August 2015.
[61]Susan Landau, 'Under the Radar: NSA's Efforts to Secure Private-sector Telecommunications Infrastructure' (2014) 7 J Nat'l Sec L & Pol'y 411, 411, 423; Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (WW Norton & Company, 2015) 119.

'easier than maintaining two versions'.[62] A further challenge to the policy emerged with the development of strong cryptographic tools by non-US companies and the fear that US companies would be disadvantaged.[63]

While export controls were gradually relaxed in the wake of powerful industry opposition,[64] government agencies continued to warn that intelligence collection was at risk of 'going dark'. One response to this concern was the passing of the Communications Assistance for Law Enforcement Act in 1994, which required all digital switch networks to be susceptible to interception.[65] The other innovation was the creation and endorsement of the Clipper initiative.

In 1993, the White House hailed the Clipper initiative as bringing the Federal Government and industry together in order to both improve telecommunications security and serve the needs of law enforcement.[66] The Clipper initiative was billed as a voluntary[67] programme that encouraged manufacturers of communications hardware to install National Security Agency (NSA) designed microcircuits into their product in order to enable government access to encrypted communications.[68] A key component of this system was the use of 'key-escrow'. According to the Presidential Directive authorising the initiative, the Attorney General would arrange for appropriate entities, with strict security procedures, to hold the keys necessary to decrypt the communications data.[69] According to the

[62]Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (WW Norton & Company, 2015) 119.

[63]Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (WW Norton & Company, 2015) 119–120.

[64]Susan Landau, 'Under the Radar: NSA's Efforts to Secure Private-sector Telecommunications Infrastructure' (2014) 7 J Nat'l Sec L & Pol'y 411, 411, 424. By the year 2000, cryptography for retail purposes was no longer subject to export controls Susan Landau, 'Under the Radar: NSA's Efforts to Secure Private-sector Telecommunications Infrastructure' (2014) 7 J Nat'l Sec L & Pol'y 411, 411, 425. Revisions to Encryption Items, 15 CFR §§ 734, 740, 742, 770, 772, and 774.

[65]Susan Landau, 'Under the Radar: NSA's Efforts to Secure Private-sector Telecommunications Infrastructure' (2014) 7 J Nat'l Sec L & Pol'y 411, 424. Communications Assistance for Law Enforcement Act, 47 USC § 229 (1994).

[66]The White House, 'White House Announcement of the Clipper Initiative' (Statement by the Press Secretary 1993) <groups.csail.mit.edu/mac/classes/6.805/articles/crypto/clipper-announcement.html> accessed 27 August 2015.

[67]While the programme was publically billed as voluntary, experts doubted the feasibility of this. Following successful Freedom of Information Act requests, EPIC reported how a briefing document sent to the National Security Council in February 1993, 'Encryption: The Threat, Applications and Potential Solutions' concluded that: 'Technical solutions, such as they are, will only work if they are incorporated into *all* encryption products. To ensure that this occurs, legislation mandating the use of Government-approved encryption products or adherence to Government encryption criteria is required'. As pointed out by then EPIC Legal Counsel David Sobel, 'the newly-disclosed information demonstrates that the architects of the Clipper program – the NSA and the FBI – have always recognized that key-escrow must eventually be mandated'. Electronic Privacy Information Center (Press Release 16 August 1995) <https://epic.org/crypto/ban/fbi_dox/press_release.html> accessed 27 August 2015. See also Electronic Privacy Information Center 'FBI Documents on Encryption' (Repository) <https://epic.org/crypto/ban/fbi_dox/> accessed 27 August 2015.

[68]Presidential Directive Authorizing the Clipper Initiative (Declassified Document Obtained by the Electronic Privacy Information Center under the Freedom of Information Act 1993) <groups.csail.mit.edu/mac/classes/6.805/articles/crypto/clipper-directive.html> accessed 27 August 2015.

[69]Presidential Directive Authorizing the Clipper Initiative (Declassified Document Obtained by the Electronic Privacy Information Center under the Freedom of Information Act 1993) <groups.csail.mit.edu/mac/classes/6.805/articles/crypto/clipper-directive.html> accessed 27 August 2015.

Directive, government agencies could only gain access to the communications where they could demonstrate appropriate legal authority to the key holders.[70]

The Clipper Chip was intended to facilitate encrypted communication while enabling government authorities to retain privileged access. In effect, the initiative created a government backdoor, but 'not a secret one. A public one'.[71] While the US government had hoped that the Clipper initiative would be a compromise solution,[72] the proposal led to wide-spread outrage amongst the technology community[73] and the initiative was eventually dropped for reasons of practicality and the First Amendment argument that computer code constitutes protected speech.[74]

The latest Crypto War

In the wake of the Snowden revelations, technology companies scrambled to rebuild trust with their customers. As the ability of technology companies to resist handing over information to the US government under secretive legal procedures was in doubt, Apple designed its newer products to prevent such a situation from arising again.[75] In all iPads and all iPhone iterations subsequent to the iPhone 3GS, Apple facilitates encryption of device content. Apple devices are encrypted in order to protect the data stored on the device (including contacts, call logs and email) against any individual who has physical access to the device but does not know the passcode necessary to decrypt it.[76]

---

[70]Presidential Directive Authorizing the Clipper Initiative (Declassified Document Obtained by the Electronic Privacy Information Center under the Freedom of Information Act 1993) <groups.csail.mit.edu/mac/classes/6.805/articles/crypto/clipper-directive.html> accessed 27 August 2015.

[71]Gordon Corera, *Intercept: The Secret History of Computers and Spies* (Weidenfeld & Nicholson, 2015) 126–127.

[72]Susan Landau, 'Under the Radar: NSA's Efforts to Secure Private-sector Telecommunications Infrastructure' (2014) 7 J Nat'l Sec L & Pol'y 411, 422; John Markoff, 'Electronics Plan Aims to Balance Government Access with Privacy' *New York Times* (New York 16 April 1993) <http://www.nytimes.com/1993/04/16/us/electronics-plan-aims-to-balance-government-access-with-privacy.html> accessed 27 August 2015. John Markoff, 'Communication Plan Draws Mixed Reaction' *New York Times* (New York 17 April 1993) <http://www.nytimes.com/1993/04/17/business/communications-plan-draws-mixed-reaction.html> accessed 27 August 2015.

[73]Steven Levy, 'Battle of the Clipper Chip' *New York Times* (New York 12 June 1994) <www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html?pagewanted=all&src=pm> accessed 27 August 2015; Gregory Ferenstein, 'How Hackers Beat The NSA In The '90s And How They Can Do It Again' *Tech Crunch* (28 June 2013) <techcrunch.com/2013/06/28/how-hackers-beat-the-nsa-in-the-90s-and-how-they-can-do-it-again/> accessed 27 August 2015.

[74]In 1999, export controls on encryption were found to be unconstitutional by the 9th Circuit Court of Appeals on First Amendment grounds. The Court stated that government efforts to control encryption 'may well implicate not only the First Amendment rights of cryptographers intent on pushing the boundaries of their science, but also the constitutional rights of each of us as potential recipients of encryption bounty'. *Bernstein v US Dep't of Justice*, 192 F 3d 1308 (9th Cir 1999), 4242. Gregory Ferenstein, 'How Hackers Beat The NSA In The '90s And How They Can Do It Again' *Tech Crunch* (28 June 2013) <techcrunch.com/2013/06/28/how-hackers-beat-the-nsa-in-the-90s-and-how-they-can-do-it-again/> accessed 27 August 2015.

[75]Craig Timberg, 'Apple will no Longer Unlock Most iPhones, iPads for Police, even with Search Warrants' *Washington Post* (Washington 18 September 2014) <www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html> accessed 27 August 2015; Jay McGregor, 'Apple Beefs Up iOS8 Security With Unbreakable Passcode' *Forbes* (18 September 2014) <www.forbes.com/sites/jaymcgregor/2014/09/18/ios8-beefs-up-security-with-unbreakable-passcode/> accessed 27 August 2015.

[76]EFF, 'How to: Encrypt Your iPhone Surveillance Self-Defense' (EFF 18 November 2014) <https://ssd.eff.org/en/module/how-encrypt-your-iphone> accessed 27 August 2015.

In September 2014, Apple boasted of its ability to thwart government data requests by designing its newer products to block Apple access to customer information.[77] In what has been described as 'an engineering solution to a legal quandary',[78] the revised Apple policy means that only the individual/consumer has access to the data stored on their Apple device. While this access was previously shared with Apple, following the updated privacy policy, Apple no longer has the ability to access this data, even when compelled to do so under a binding legal order.[79] The economic and public relations interest in this announcement was underlined by the statement from Apple that 'unlike our competitors, Apple cannot bypass your passcode and therefore cannot access this data'.[80] The policy change was well-received by privacy advocates, security experts, and consumers.[81] Accordingly, it was unsurprising when Google followed with similar pledges.[82]

[77]Craig Timberg, 'Apple will no Longer Unlock Most iPhones, iPads for Police, even with Search Warrants' *Washington Post* (Washington 18 September 2014) <www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html> accessed 27 August 2015; Jay McGregor, 'Apple Beefs Up iOS8 Security With Unbreakable Passcode' *Forbes* (18 September 2014) <www.forbes.com/sites/jaymcgregor/2014/09/18/ios8-beefs-up-security-with-unbreakable-passcode/> accessed 27 August 2015. It is important to note that any data uploaded to cloud services can still be retrievable through legal warrants. John Leyden, 'Apple Slaps a Passcode Lock on iOS 8 Devices, but Cops can still Inhale your iCloud' *The Register* (23 September 2014) <www.theregister.co.uk/2014/09/23/icloud_hole_in_ios8_passcode_protection/> accessed 27 August 2015; In addition, while the new system has been praised by experts, remaining vulnerabilities have also been identified. Jonathan Zdziarski, 'Your iOS 8 Data is Not Beyond Law Enforcement's Reach … Yet' *Zdziarski's Blog of Things* (17 September 2014) <www.zdziarski.com/blog/?p=3875> accessed 27 August 2015.

[78]Craig Timberg, 'Apple will no Longer Unlock Most iPhones, iPads for Police, even with Search Warrants' *Washington Post* (Washington 18 September 2014) <www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html> accessed 27 August 2015; Jay McGregor, 'Apple Beefs Up iOS8 Security With Unbreakable Passcode' *Forbes* (18 September 2014) <www.forbes.com/sites/jaymcgregor/2014/09/18/ios8-beefs-up-security-with-unbreakable-passcode/> accessed 27 August 2015.

[79]Jay McGregor, 'Apple Beefs Up iOS8 Security With Unbreakable Passcode' *Forbes* (18 September 2014) <www.forbes.com/sites/jaymcgregor/2014/09/18/ios8-beefs-up-security-with-unbreakable-passcode/> accessed 27 August 2015.

[80]Jay McGregor, 'Apple Beefs Up iOS8 Security With Unbreakable Passcode' *Forbes* (18 September 2014) <www.forbes.com/sites/jaymcgregor/2014/09/18/ios8-beefs-up-security-with-unbreakable-passcode/> accessed 27 August 2015.

[81]Kevin Poulsen, 'Apple's iPhone Encryption Is a Godsend, Even if Cops Hate It' *Wired* (8 October 2014) <www.wired.com/2014/10/golden-key/> accessed 27 August 2015; Open letter from Civil Society Organizations Companies and Trade Associations Security and Policy Experts to President Obama (19 May 19 2015) <https://static.newamerica.org/attachments/3138–113/Encryption_Letter_to_Obama_final_051915.pdf> accessed 27 August 2015; Adam Clark Estes, 'Cops Have No Right to Be Angry About the iPhone's New Encryption' *Gizmodo* (23 September 2014) <gizmodo.com/cops-have-no-right-to-be-angry-about-apples-improved-se-1638256237> accessed 27 August 2015; Iain Thomson, 'FBI Boss: Apple's iPhone, iPad Encryption puts People "Above the Law"' *The Register* (25 September 2014) <www.theregister.co.uk/2014/09/25/fbi_boss_slams_google_apple_for_encryption_that_puts_users_above_law/> accessed 27 August 2015; Bruce Schneier, 'Stop the Hysteria over Apple Encryption' *Schneier on Security* (3 October 2014) <https://www.schneier.com/essays/archives/2014/10/stop_the_hysteria_ov.html> accessed 27 August 2015; Jennifer Abel, 'Privacy Advocates and Tech Giants Support Encryption, which the FBI Director finds "Depressing"' *Consumer Affairs* (21 May 2015) <www.consumeraffairs.com/news/privacy-advocates-and-tech-giants-support-encryption-which-the-fbi-director-finds-depressing-052115.html> accessed 27 August

[82]Darren Pauli, 'Google Apple Grapple brings Crypto Cop Block to Android' *The Register* (19 September 2014) <www.theregister.co.uk/2014/09/19/google_apple_grapple_brings_crypto_cop_block_to_android/> accessed 27 August.

While investigative authorities have long bemoaned the obstacles created by encryption, the Apple policy change incited heightened debate on the topic. The Federal Bureau of Investigation's (FBI's) James Comey railed against Apple's announcement and criticised the use of such encryption systems generally.[83] Comey warned that the popularisation of encryption technologies 'threatens to lead us all to a very, very dark place'.[84] Such warnings are reminiscent of statements made during the original Crypto War. Testifying before Congress in 1995, then Director of the FBI, Louis Freeh, stated that public-key encryption 'jeopardizes the public safety and national security of this country'.[85] According to Comey, companies who are currently not subject to the US Communications Assistance for Law Enforcement Act should be compelled to build 'lawful intercept capabilities for law enforcement'.[86] Such access would require security 'back doors' to be built into technology services and products that provide encryption. According to its updated privacy policy, Apple would be technologically unable to compromise its customers' privacy in this manner.

Since Comey's initial statements, he has testified before Senate Committees on this issue. While Comey maintains his position that exceptional government access is necessary, he provides no further detail as to how such access could be safely granted.[87] Even broadly described proposals for what a system of exceptional government access to communications should look like vary in their details. For example, the director of the NSA, Michael Rogers, has argued that 'back door' is an inappropriate term in this context and that investigative authorities are actually seeking 'front door' access. By this, Rogers draws attention to the fact that in their public statements, investigative agency representatives have only called for exceptional access on foot of appropriate legal authority. While this is primarily an issue of semantics, Rogers has extended the metaphor and has argued that the ideal system would have multiple locks.[88] This is a reference to split-key

[83]Igor Bobic and Ryan Reilly, 'FBI Director James Comey "Very Concerned" About New Apple, Google Privacy Features' *Huffington Post* (25 September 2014) <www.huffingtonpost.com/2014/09/25/james-comey-apple-encryption_n_5882874.html> accessed 27 August.

[84]James Comey, 'Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?' (Speech at the Brookings Institute, Washington DC, 2014) <https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course> accessed 27 August; Spencer Ackerman, 'FBI Director Attacks Tech Companies for Embracing New Modes of Encryption' *The Guardian* (London 16 October 2014) <www.theguardian.com/us-news/2014/oct/16/fbi-director-attacks-tech-companies-encryption> accessed 27 August.

[85]Freeh argued that 'Drug cartels, terrorists, and kidnappers will use telephones and other communications media with impunity knowing that their conversations are immune' from interception. Charles Mann, 'Homeland Insecurity' *The Atlantic Monthly* (Washington 28 June 2002) <www.charlesmann.org/articles/Homeland-Insecurity-Atlantic.pdf> accessed 27 August.

[86]James Comey, 'Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?' (Speech at the Brookings Institute, Washington DC, 2014) <https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course> accessed 27 August; Spencer Ackerman, 'FBI Director Attacks Tech Companies for Embracing New Modes of Encryption' *The Guardian* (London 16 October 2014) <www.theguardian.com/us-news/2014/oct/16/fbi-director-attacks-tech-companies-encryption> accessed 27 August.

[87]Jenna McLaughlin, 'FBI Director Says Scientists Are Wrong, Pitches Imaginary Solution to Encryption Dilemma' *The Intercept* (8 July 2015) <https://firstlook.org/theintercept/2015/07/08/fbi-director-comey-proposes-imaginary-solution-encryption/> accessed 27 August.

[88]Ellen Nakashima and Barton Gellman, 'As Encryption Spreads, US Grapples with Clash between Privacy, Security)' *Washington Post* (Washington 10 April 2015) <https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html> accessed 27 August.

systems which allow for the creation of a digital key but separates that key 'so that no one person or agency alone' has the sole power to use it.[89]

Whether using the term back door or front door, however, security experts agree that the creation of special access to encrypted information constitutes the creation of intentional vulnerabilities in encryption systems.[90] While there is some intuitive appeal to the concept that governments should be able to gain special access to communications in order to prevent crime, the security community have highlighted the impossible promise of a 'golden key' solution.[91] The reason such a solution is not possible is because 'any vulnerability in an information system may be exploited by criminals and law enforcement agencies in equal measure'.[92] As much as one might wish there was a 'golden key' solution that would permit lawful government access to encrypted information without compromising Internet communications, no such solution has ever been identified.[93] Eric Schmidt of Google summed up this position when he stated that,

> [i]f we put a trap door in our system, first, we would have to disclose it because people would find out anyway. And second, some evil person in addition to the good guys would figure out a way to get in.[94]

[89]Ellen Nakashima and Barton Gellman, 'As Encryption Spreads, US Grapples with Clash between Privacy, Security' *Washington Post* (Washington 10 April 2015) <https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html> accessed 27 August.

[90]Harold Abelson and others, 'Keys Under Doormats: Mandating Insecurity by Requiring Government Access to all Data and Communications' (Computer Science and Artificial Intelligence Laboratory Technical Report 2015) <dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8> accessed 27 August.

[91]Editorial, 'Compromise Needed on Smartphone Encryption' *Washington Post* (Washington 3 October 2014) <https://www.washingtonpost.com/opinions/compromise-needed-on-smartphone-encryption/2014/10/03/96680bf8-4a77-11e4-891d-713f052086a0_story.html> accessed 27 August; Jeremy Gillula, 'Even a Golden Key Can Be Stolen by Thieves: The Simple Facts of Apple's Encryption Decision' *Electronic Frontier Foundation* (10 October 2014) <https://www.eff.org/deeplinks/2014/10/even-golden-key-can-be-stolen-thieves-simple-facts-apples-encryption-decision> accessed 27 August; Mike Masnick, 'Washington Post's Clueless Editorial On Phone Encryption: No Backdoors, But How About A Magical "Golden Key"?' *Tech Dirt* (6 October 2014) <https://www.techdirt.com/articles/20141006/01082128740/washington-posts-braindead-editorial-phone-encryption-no-backdoors-how-about-magical-golden-key.shtml> accessed 27 August.

[92]Article 19, 'Response to UN Special Rapporteur's Call for Comments on Encryption and Anonymity' (Submission February 2015) 14 <www.ohchr.org/Documents/Issues/Opinion/Communications/Article19.pdf> accessed 27 August 2015; Jeremy Gillula, 'Even a Golden Key Can Be Stolen by Thieves: The Simple Facts of Apple's Encryption Decision' *Electronic Frontier Foundation* (10 October 2014) <https://www.eff.org/deeplinks/2014/10/even-golden-key-can-be-stolen-thieves-simple-facts-apples-encryption-decision> accessed 27 August.

[93]Article 19, 'Response to UN Special Rapporteur's Call for Comments on Encryption and Anonymity' (Submission February 2015) <www.ohchr.org/Documents/Issues/Opinion/Communications/Article19.pdf> accessed 27 August 2015; Jeremy Gillula, 'Even a Golden Key Can Be Stolen by Thieves: The Simple Facts of Apple's Encryption Decision' *Electronic Frontier Foundation* (10 October 2014) <https://www.eff.org/deeplinks/2014/10/even-golden-key-can-be-stolen-thieves-simple-facts-apples-encryption-decision> accessed 27 August.

[94]AFP, 'Tech Firms "Will Win" Encryption Battle: Google Chief' *Security Week* (18 March 2015) <www.securityweek.com/tech-firms-will-win-encryption-battle-google-chief> accessed 27 August; Editorial, 'Compromise Needed on Smartphone Encryption' *Washington Post* (Washington 3 October 2014) <https://www.washingtonpost.com/opinions/compromise-needed-on-smartphone-encryption/2014/10/03/96680bf8-4a77-11e4-891d-713f052086a0_story.html> accessed 27 August.

With no specific technological solution currently being proposed, technology companies and security experts remain at odds with law enforcement and surveillance interests. In July 2015, the Washington Post pointed out that Silicon Valley and Washington 'have spent the past year arguing over whether technology companies should enable users to encrypt their digital lives in such a way that not even the Federal Bureau of Investigation could unscramble the information'.[95] While President Obama has made some supportive statements,[96] he has admitted to leaning 'probably further in the direction of strong encryption than some do inside of law enforcement'.[97] It has been argued that there is 'zero chance' of any anti-encryption legislation being passed by the US Congress absent a 'catastrophic event which clearly could have been stopped if the government had been able to break some encryption'.[98] Accordingly, while there is strong support for new law amongst US law enforcement and surveillance authorities, legislation mandating exceptional access is unlikely in the immediate future.

The situation appears different in the UK where David Cameron has yet to back down from his 2015 General Election pledges strongly opposed to consumer encryption.[99] Cameron has stated that he believes it should always be possible to gain access to communications where the Home Secretary has signed a warrant.[100] In a response to a question in Parliament in June 2015, Cameron maintained the pre-election campaign position, arguing that the government simply wants to ensure that 'terrorists do not have a safe space in which to communicate'.[101]

[95]Danny Yadron, Damian Paletta, and Jennifer Valentino-Devries, 'Technology Experts Hit Back at FBI on Encryption' *Wall Street Journal* (New York 7 July 2015) <http://www.wsj.com/articles/technology-experts-hit-back-at-fbi-on-encryption-1436316464> accessed 27 August.

[96]Nicholas Watt and others, 'David Cameron Pledges Anti-Terror Law for Internet after Paris Attacks' *The Guardian* (London 12 January 2015) <www.theguardian.com/uk-news/2015/jan/12/david-cameron-pledges-anti-terror-law-internet-paris-attacks-nick-clegg> accessed 27 August and James Comey, 'Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?' (Speech at the Brookings Institute, Washington DC, 2014) <https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course> accessed 27 August.

[97]Ellen Nakashima and Barton Gellman, 'As Encryption Spreads, US Grapples with Clash between Privacy, Security' *Washington Post* (Washington 10 April 2015) <https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html> accessed 27 August.

[98]Ellen Nakashima and Barton Gellman, 'As Encryption Spreads, US Grapples with Clash between Privacy, Security' *Washington Post* (Washington 10 April 2015) <https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html> accessed 27 August.

[99]Ian Johnston, 'David Cameron Pledges New "Snoopers' Charter" if he Wins General Election' *Independent* (London 12 January 2015) <www.independent.co.uk/news/uk/politics/david-cameron-pledges-new-snoopers-charter-if-he-wins-election-9971379.html> accessed 27 August; James Comey, 'Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?' (Speech at the Brookings Institute, Washington DC, 2014) <https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course> accessed 27 August.

[100]Ian Johnston, 'David Cameron Pledges New "Snoopers' Charter" if he Wins General Election' *Independent* (London 12 January 2015) <www.independent.co.uk/news/uk/politics/david-cameron-pledges-new-snoopers-charter-if-he-wins-election-9971379.html> accessed 27 August; Rob Price, 'David Cameron Wants To Ban Encryption' *Business Insider* (12 January 2015) <uk.businessinsider.com/david-cameron-encryption-apple-pgp-2015-1> accessed 27 August; James Comey, 'Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?' (Speech at the Brookings Institute, Washington DC, 2014) <https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course> accessed 27 August.

[101]Adam Bienkov, 'David Cameron: Twitter and Facebook Privacy is Unsustainable' *Politics.co.uk* (30 June 2015) <www.politics.co.uk/news/2015/06/30/david-cameron-twitter-and-facebook-privacy-is-unsustainable> accessed 27 August.

Reiterating his election statements, Cameron stated that the government must consider all new media and ensure that the authorities are always able to 'on the signature of a warrant, to get to the bottom of what is going on'.[102] While it should be noted that a spokesperson has since stated that the Prime Minister accepts and recognises the importance of encryption and has no plans to outlaw it completely, the same spokesperson's reiteration that the British government believes 'terrorists cannot have a safe space in which to operate' online undermines the significance of the initial reassurance.[103]

Interplay of interests

Adopting the position that strong encryption is an essential privacy tool in the modern world, it is necessary to investigate how the use of such technology can be protected. In order to assess the best available options, it is necessary to consider, once again, our primary stakeholders: governments, technology companies, individuals/consumers, and security experts. It is sensible to consider how the legitimate interests and incentives of these major parties should influence policy in this area. First and foremost, it is clear that all four parties have an incentive to protect the security of information.[104] This common incentive is a boon to privacy as security is an essential precondition to privacy. In addition to the common interest in information security, an overlapping interest in privacy protection exists between the individual and technology companies, if only because privacy encourages greater use and uptake of technological products and services. Following the anti-encryption remarks from David Cameron, several technology companies have threatened to take their business out of the UK.[105] Even though Comey recognises the economic cost of building government access into communications products and services, Comey maintains that American companies should be forced to modify their products.[106] While Comey acknowledges that companies based in other countries might gain a competitive advantage, he believes that American companies should be willing to 'take that hit'.[107]

[102]Adam Bienkov, 'David Cameron: Twitter and Facebook Privacy is Unsustainable' *Politics.co.uk* (30 June 2015) <www.politics.co.uk/news/2015/06/30/david-cameron-twitter-and-facebook-privacy-is-unsustainable> accessed 27 August.

[103]Rob Price, 'The UK Government Insists it's Not Going to Try and Ban Encryption' *Business Insider* (14 July 2015) <http://uk.businessinsider.com/uk-government-not-going-to-ban-encryption-2015-7?r=US#ixzz3gdX6ACWY> accessed 27 August.

[104]Interestingly, the COMSEC branch of the NSA has as its explicit function the protection of communications security Susan Landau, 'Under the Radar: NSA's Efforts to Secure Private-sector Telecommunications Infrastructure' (2014) 7 J Nat'l Sec L & Pol'y 411, 411.

[105]Alison Powell, 'The Government's Investigatory Powers Bill may mean Digital Innovators say Bye to Britain' *LSE Blog* <blogs.lse.ac.uk/politicsandpolicy/the-governments-proposed-investigatory-powers-bill-may-mean-digital-innovators-say-bye-to-britain/?utm_content=buffer1f9e4&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer> accessed 27 August.

[106]James Comey, 'Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?' (Speech at the Brookings Institute, Washington DC, 2014) <https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course> accessed 27 August; Spencer Ackerman, 'FBI Director Attacks Tech Companies for Embracing New Modes of Encryption' *The Guardian* (London 16 October 2014) <www.theguardian.com/us-news/2014/oct/16/fbi-director-attacks-tech-companies-encryption> accessed 27 August.

[107]James Comey, 'Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?' (Speech at the Brookings Institute, Washington DC, 2014) <https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course> accessed 27 August; Spencer Ackerman, 'FBI Director Attacks Tech Companies for Embracing New Modes of

Supporting the argument for strong encryption, therefore, are both security and economic factors. In spite of clear potential for economic and security harm, continued support in some quarters for weakened encryption security indicates a strong – perhaps overriding – government interest in the unencumbered conduction of surveillance. In spite of the expressed desire to weaken encryption systems in order to enable government access, there is an argument to be made that a secure system, based on strong encryption, is more important for technologically and economically advanced countries than to other countries. As pointed out by Edward Snowden, there seems to be little sense in the US policy – the country with the biggest vault of valuable information to lose – to be lowering the standards of vaults worldwide.[108] Similar arguments could be made in the UK context.

Such reasoning echoes the opinions of security experts who, for many years, have argued against granting any exceptional access to government agencies.[109] Of particular note is a recent report written by an expert group of security technologists.[110] The authors of this report include such security luminaries as Whitfield Diffie, Ronald Rivest, and Bruce Schneier. The report states that granting back door access to governments will 'open doors through which criminals and malicious nation-states can attack the very individuals law enforcement seeks to defend'.[111] According to the report, 'the costs would be substantial, the damage to innovation severe, and the consequences to economic growth difficult to predict'.[112]

In spite of their great interest in security, certain sections of the US and UK governments[113] still pursue anti-encryption policies – through technological exploitation and sabotage as well as proposals for encryption inhibiting laws.[114] These policies indicate

Encryption' *The Guardian* (London 16 October 2014) <www.theguardian.com/us-news/2014/oct/16/fbi-director-attacks-tech-companies-encryption> accessed 27 August.

[108]Cory Doctorow, 'Edward Snowden: "The NSA Set Fire to the Internet. You are the Firefighters' *The Guardian* (London 11 March 2014) <www.theguardian.com/technology/2014/mar/11/edward-snowden-sxsw-nsa-internet> accessed 27 August.

[109]Ronald Rivest, 'The Case against Regulating Encryption Technology' *Scientific American* (October 1998) <https://people.csail.mit.edu/rivest/pubs/Riv98e.pdf> accessed 27 August 2015;Steven Levy, 'Battle of the Clipper Chip' *New York Times* (New York 12 June 1994) <www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html?pagewanted=all&src=pm> accessed 27 August 2015; Lynn McNulty, 'Encryption's Importance to Economic and Infrastructure Security' (1998–1999) 9 Duke J Comp & Int'l L 427, 440; Ryan Singel, 'FBI Drive for Encryption Backdoors is Déjà Vu for Security Experts' *Ars Technica* (28 September 2010) <arstechnica.com/tech-policy/2010/09/fbi-drive-for-encryption-backdoors-is-deja-vu-for-security-experts/> accessed 27 August 2015.

[110]Harold Abelson and others, 'Keys Under Doormats: Mandating Insecurity by Requiring Government Access to all Data and Communications' (Computer Science and Artificial Intelligence Laboratory Technical Report 2015) <dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8> accessed 27 August.

[111]Harold Abelson and others, 'Keys Under Doormats: Mandating Insecurity by Requiring Government Access to all Data and Communications' (Computer Science and Artificial Intelligence Laboratory Technical Report 2015) 24–25. <dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8> accessed 27 August.

[112]Harold Abelson and others, 'Keys Under Doormats: Mandating Insecurity by Requiring Government Access to all Data and Communications' (Computer Science and Artificial Intelligence Laboratory Technical Report 2015) 24–25 <dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8> accessed 27 August.

[113]Along with many other countries.

[114]Nicole Perlroth, Jeff Larson, and Scott Shane, 'NSA able to Foil Basic Safeguards of Privacy on Web' *New York Times* (New York 5 September 2013) <www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all&_r=0> accessed 27 August; Editorial, 'Close the

a willingness on the part of governments to trade a degree of security for perceived intelligence benefits. This preference should not be ignored. If policy is to be influenced, the real incentives and interests of the parties should be recognised and better – more protective – solutions sought. Accordingly, it is important to look for alternative incentives and to consider how else government policy can be influenced. This calls for consideration of what the appropriate role of law is in this area and requires the investigation of how to best conceptualise arguments in favour of enhanced security and by implication privacy.

Human right to encryption?

As economic and information security arguments have failed to convince government authorities to fully support encryption, it is reasonable to consider whether a human rights obligation could be identified in order to compel such support, or perhaps, more realistically, to limit the extent to which governments interfere with encryption standards. The concept of encryption as a human right has received increased attention recently, most notably in the report of David Kaye for the United Nations.[115] In his report, Kaye concluded that 'States should adopt policies of non-restriction or comprehensive protection' towards encryption and anonymity and States should only impose restrictions on these tools on a case-specific basis.[116] As a human right to encryption is not found in international texts in the same manner as the right to privacy is, the question becomes whether encryption is essential for the protection of other rights.

From the European Convention on Human Rights (ECHR) perspective it is clear that Article 10 ECHR and Article 8 ECHR are likely to be most relevant to the issue of encryption. The structure of these rights is quite similar with the first paragraph of Article 8 ECHR guaranteeing the right to respect for private and family life and the first paragraph of Article 10 ECHR protecting freedom of expression. Freedom of expression includes the freedom to 'hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers'.[117] Both Articles 8 and 10 ECHR are limited by similarly phrased second paragraphs.[118] Article 8 ECHR may be interfered with where the interference is 'in accordance with the law',

> necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[119]

NSA's Back Doors' *New York Times* (New York 21 September 2013) <http://www.nytimes.com/2013/09/22/opinion/sunday/close-the-nsas-back-doors.html?_r=0> accessed 27 August.

[115]Human Rights Council, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye' (2015) UN Doc A/HRC/29/3.

[116]Human Rights Council, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye' (2015) UN Doc A/HRC/29/3, 19.

[117]Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR) art 10.

[118]Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR) arts 10(2) and 8(2).

[119]Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR) art 8(2).

Similarly, Article 10 ECHR may be limited where restrictions are 'prescribed by law', 'necessary in a democratic society' and

> in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.[120]

Freedom of expression and privacy are integrally linked in a democratic society.[121] When an individual does not enjoy privacy, their freedom of expression can be inhibited, for example, by encouraging individuals to self-censor.[122] As history provides many examples of surveillance being abused to control dissenters in times of supposed emergency, the importance of secure communications is clear.[123] The link between privacy and freedom of expression was acknowledged by the Committee of Ministers of the Council of Europe in a 2003 declaration that called on Member States to respect the desire of Internet users to conceal their identity.[124] The Committee of Ministers stated that protection against surveillance and the enhancement of free expression required States to 'respect the will of users of the Internet not to disclose their identity'.[125] This stance recognises that individuals will be less likely to gather information and to formulate and discuss ideas if they suspect that they are being watched.

In order to begin thinking about whether encryption is a necessary aspect of privacy and/or free expression rights, it is important to consider what encryption is in a conceptual

[120]Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR) art 10(2).

[121]Human Rights Council, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue' (2013) UN Doc A/HRC/23/40.

[122]Daniel Solove, 'A Taxonomy of Privacy' (2006) 154 U Pa L Rev 477, 491–499; Edward Long, *The Intruders* (Praeger, 1967) viii. As referenced in Stanley Benn, 'Privacy, Freedom, and Respect for Persons' in Ferdinand Schoeman (ed), *Philosophical Dimensions of Privacy* (CUP, 1984) 304; Walter Peissl, *Surveillance and Security – A Dodgy Relationship* (Institute of Technology Assessment Manuscript, 2002) 8 <http://www.oeaw.ac.at/ita/pdf/ita_02_02.pdf> accessed 27 August. See also, David Lyon, 'Surveillance, power, and everyday life' in Robin Mansell and others (eds), *The Oxford Handbook of Information and Communication Technologies* (OUP, 2009) 452. The 'chilling effect' doctrine postulates that even where individual measures of surveillance are carried out on a covert basis, general awareness of the possibility of surveillance fosters suspicion amongst the population. This suspicion is prone to manifest itself in a hesitance to share views that could be perceived as subversive. See Frederick Schauer, 'Fear, Risk and the First Amendment: Unraveling the Chilling Effect' (1978) 58 BUL Rev 685, 690.

[123]A famous example is provided by The Church Committee, which reported in 1976 that every President from Roosevelt to Nixon improperly used government surveillance to obtain information about critics and political opponents. US Senate, *Hearings Before the Select Committee to Study Governmental Operations with Respect to Intelligence Activities,* 94th Congress (April 14 1976) 5 <http://www.archive.org/stream/finalreportofsel01unit/finalreportofsel01unit_djvu.txt> accessed 27 August; Alan Westin, *Privacy and Freedom* (Atheneum, 1967) 368.

[124]Council of Europe, 'Committee of Ministers Declaration on Freedom of Communication on the Internet' (Adopted by the Committee of Ministers 2003) Principle 7 <https://wcd.coe.int/ViewDoc.jsp?id=37031> accessed 27 August.

[125]Council of Europe, 'Committee of Ministers Declaration on Freedom of Communication on the Internet' (Adopted by the Committee of Ministers 2003) Principle 7 <https://wcd.coe.int/ViewDoc.jsp?id=37031> accessed 27 August.

sense. Is encryption a munition, a tool for terrorists and criminals,[126] or is encryption something else? It is contended that, at its core, encryption protects the sanctity of an individual's thoughts, communications, and in some cases, their anonymity.[127]

As Article 8 ECHR guarantees respect for correspondence[128] and private life,[129] government interference with encryption – a key tool used by many to protect the security of communications – clearly requires consideration of the Article.[130] In addition to protecting the content of communications, Article 10 ECHR also protects 'the means of transmission or reception' of communications. The European Court of Human Rights (ECtHR) has held that any restriction on the means of communication 'necessarily interferes with the right to receive and impart information'.[131] As encryption is an essential tool chosen by many who wish to communicate securely, it seems clear that government interference with encryption also requires scrutiny under Article 10 ECHR.

While government interference with encryption will require consideration of privacy and free expression rights, the second paragraphs of Articles 8 and 10 ECHR clearly indicate the non-absolute nature of these rights. Similarly, the Committee of Ministers has recognised that the importance of anonymity does not prevent Member States

> from taking measures and co-operating in order to trace those responsible for criminal acts, in accordance with national law, the Convention for the Protection of Human Rights and Fundamental Freedoms and other international agreements in the fields of justice and the police.[132]

In a non-encryption context, the ECtHR has adopted a cautious approach when considering the existence of a right to online anonymity. While the ECtHR in *KU v Finland* linked anonymity to privacy and free expression, the Court also highlighted the limited nature of the right by pointing out that 'such guarantees cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection

[126]Indeed, the Chief of Detectives for the Chicago Police Department, John Escalante, argued that 'Apple will become the phone of choice for the pedophile'. Tim Cushing, 'Another Police Chief says Phone Encryption is a Pedophile's Best Friend' *Tech Dirt* (2 October 2014) <https://www.techdirt.com/articles/20140930/13125228682/another-police-chief-says-phone-encryption-is-pedophiles-best-friend.shtml> accessed 27 August.

[127]See Human Rights Council, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye' (2015) UN Doc A/HRC/29/3, 8-9.

[128]The ECtHR accepts that correspondence should include electronic communication. *Halford v The United Kingdom* [1997] 24 EHRR 523.

[129]The European Court of Human Rights has stated that the right to respect for private life is a 'broad term not susceptible to exhaustive definition'. The Convention Organs have found the right to respect for private life to encompass a broad range of circumstances. *Peck v The United Kingdom* (2003) 36 EHRR 41 [57]; *Niemietz v Germany* (1992) 16 EHRR 97 [29]; *Pretty v The United Kingdom* [2002] ECHR 427 [61]; *PG and JH v The United Kingdom* [2001] ECHR 550 [56]; *X v Iceland* [1976] 5 D and R 86 [87]; *Rotaru v Romania* [2000] ECHR 192 [43]; *Amann v Switzerland* (2000) 30 EHRR 843 [65]; *von Hannover v Germany* (2005) 40 EHRR 1 [50].

[130]Human Rights Council, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye' (2015) UN Doc A/HRC/29/3, 19.

[131]*Autronic AG v Switzerland* [1990] ECHR 12 [47].

[132]Council of Europe, 'Committee of Ministers Declaration on Freedom of Communication on the Internet' (Adopted by the Committee of Ministers 2003) Principle 7 <https://wcd.coe.int/ViewDoc.jsp?id=37031> accessed 27 August.

of the rights and freedoms of others'.[133] Similarly, in a case concerning the obligations of Internet news portals (*Delfi AS v Estonia*), the Grand Chamber argued that anonymity on the Internet is an important value, but must be balanced against other rights and interests.[134] While not directly concerned with encryption, the cases of *KU v Finland* and *Delfi AS v Estonia* are of assistance when attempting to assess how the ECtHR might view State restriction of encryption standards as similar tensions are embodied in the encryption debate.

As restrictions on encryption could clearly hinder the receipt and imparting of information without interference by public authorities[135] and restrictions could also constitute an interference by public authorities in the private life of individuals,[136] any legislation restricting encryption would have to be deemed to be prescribed by law and necessary in a democratic society in the pursuit of a legitimate aim. In light of this conclusion, it is necessary to consider how Article 8 ECHR and Article 10 ECHR might apply to recent activities of US and UK intelligence agencies.

It is clear that intelligence agencies have made many covert efforts to restrict encryption. Documents released by Snowden indicate the existence of a major NSA decryption program, codenamed as Bullrun.[137] According to the documents released, the purpose of the Bullrun program is to 'defeat the encryption used in specific network communication technologies'.[138] These documents were leaked to the New York Times, which reported that the NSA was 'winning its long-running secret war on encryption, using supercomputers, technical trickery, court orders and behind-the-scenes persuasion to undermine the major tools protecting the privacy of everyday communications in the Internet age'.[139] Unsurprisingly, GCHQ developed its own comparable anti-encryption program, codenamed 'Edgehill'.[140]

---

[133] *KU v Finland* [2008] ECHR 1563 [49]; Article 19, 'Response to UN Special Rapporteur's Call for Comments on Encryption and Anonymity' (Submission February 2015) 8 <www.ohchr.org/Documents/Issues/Opinion/Communications/Article19.pdf> accessed 27 August 2015.

[134] *Delfi AS v Estonia* [2015] ECHR 586 [161] citing *KU v Finland* [2008] ECHR 1563 [49].

[135] As protected by Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR) art 10.

[136] As protected against by Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR) art 8.

[137] ____, 'Project Bullrun – Classification Guide to the NSA's Decryption Program' *The Guardian* (London 5 September 2013) <www.theguardian.com/world/interactive/2013/sep/05/nsa-project-bullrun-classification-guide> accessed 27 August.

[138] ____, 'Project Bullrun – Classification Guide to the NSA's Decryption Program' *The Guardian* (London 5 September 2013) <www.theguardian.com/world/interactive/2013/sep/05/nsa-project-bullrun-classification-guide> accessed 27 August; The National Institute of Standards and Technology. Nicole Perlroth, Jeff Larson, and Scott Shane, 'NSA able to Foil Basic Safeguards of Privacy on Web' *New York Times* (New York 5 September 2013) <www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all&_r=0> accessed 27 August; Editorial, 'Close the NSA's Back Doors' *New York Times* (New York 21 September 2013) <http://www.nytimes.com/2013/09/22/opinion/sunday/close-the-nsas-back-doors.html?_r=0> accessed 27 August.

[139] Nicole Perlroth, Jeff Larson, and Scott Shane, 'NSA able to Foil Basic Safeguards of Privacy on Web' *New York Times* (New York 5 September 2013) <www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all&_r=0> accessed 27 August; Editorial, 'Close the NSA's Back Doors' *New York Times* (New York 21 September 2013) <http://www.nytimes.com/2013/09/22/opinion/sunday/close-the-nsas-back-doors.html?_r=0> accessed 27 August.

[140] James Ball, Julian Borger, and Glenn Greenwald, 'Revealed: how US and UK Spy Agencies Defeat Internet Privacy and Security' *The Guardian* (London 6 September 2013) <http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security> accessed 27 August.

A key feature of these programs was the scrupulous commitment to secrecy. Leaked documents revealed how reports 'generated from BULLRUN-derived information' were not to reveal 'BULLRUN details'.[141] GCHQ analysts were instructed to neither 'ask about' nor 'speculate on sources or methods underpinning Bullrun'.[142] On the test of legality it seems clear that the surreptitious anti-encryption activities of surveillance agencies as exposed in the Snowden revelations would fail to meet the requirement of legality under the Convention. When assessing whether an intrusive measure meets the test of legality, the ECtHR asks whether the measure has 'some basis in domestic law',[143] whether the law is adequately accessible,[144] and whether the requirement of foreseeability has been met.[145] The rule of law requires that domestic surveillance law protects against 'arbitrary interference' by government authorities with the rights of individuals.[146] Assiduousness to this principle is particularly important where the government exercises power in secret as when actions are obscured from public scrutiny, there is an increased risk of arbitrariness.[147]

To take one particularly egregious example, consider the SIM card scandal, most associated with the company Gemalto.[148] According to documents released by Snowden and reported on by the Intercept, the NSA and GCHQ hacked into Gemalto systems in order to steal the SIM card encryption keys used to protect the privacy of mobile phone communications.[149] As pointed out by the Intercept, access to SIM card encryption keys enables direct access to mobile communications without the need to seek legal authority or cooperation from telecommunications companies.[150] Even though Gemalto dispute

[141]——, 'Project Bullrun – Classification Guide to the NSA's Decryption Program' *The Guardian* (London 5 September 2013) <www.theguardian.com/world/interactive/2013/sep/05/nsa-project-bullrun-classification-guide> accessed 27 August.

[142]See ——, 'BULLRUN' (Leaked GCHQ presentation) <https://www.eff.org/files/2015/01/28/20141228-spiegel-gchq_presentation_on_the_bullrun_programs_decryption_capabilities.pdf> accessed 27 August; James Ball, Julian Borger, and Glenn Greenwald, 'Revealed: how US and UK Spy Agencies Defeat Internet Privacy and Security' *The Guardian* (London 6 September 2013) <http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security> accessed 27 August.

[143]*Silver v The United Kingdom* [1983] ECHR 5 [86] citing *Sunday Times v The United Kingdom* (1979–80) 2 EHRR 245 [47]. For example, an inadequate legal basis for surveillance activities was identified by the ECtHR in *Malone v The United Kingdom* [1984] ECHR 10 [79]; *Khan v The United Kingdom* (2000) 31 EHRR 45 [27]-[28]; *Allan v The United Kingdom* [2002] ECHR 702 [36]; and *Copland v The United Kingdom* (2007) 45 EHRR 37 [48].

[144]*Liberty v The United Kingdom* [2008] ECHR 568 [69].

[145]Laws must indicate the scope of the discretion allowed to government authorities and must indicate how that discretion can be exercised with 'sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference'. *Malone v The United Kingdom* [1984] ECHR 10 [68].

[146]See, for example, *Valenzuela Contreras v Spain* (1999) 28 EHRR 483 [46] and *Kopp v Switzerland* (1998) 27 EHHR 93 [64].

[147]See, for example, *Malone v The United Kingdom* [1984] ECHR 10 [67]; *Klass v Germany* (1979–80) 2 EHRR 214 [42]-[49]; and *Ekimdzhiev v Bulgaria* [2007] ECHR 533 [71].

[148]Jeremy Scahill and Josh Begley, 'The Great Sim Heist: How Spies Stole the Keys to the Encryption Castle' *The Intercept* (10 February 2015) <https://firstlook.org/theintercept/2015/02/19/great-sim-heist> accessed 27 August.

[149]Jeremy Scahill and Josh Begley, 'The Great Sim Heist: How Spies Stole the Keys to the Encryption Castle' *The Intercept* (10 February 2015) <https://firstlook.org/theintercept/2015/02/19/great-sim-heist> accessed 27 August.

[150]Jeremy Scahill and Josh Begley, 'The Great Sim Heist: How Spies Stole the Keys to the Encryption Castle' *The Intercept* (10 February 2015) <https://firstlook.org/theintercept/2015/02/19/great-sim-heist> accessed 27 August.

whether encryption keys were successfully stolen, the company investigation[151] did identify unauthorised activity in the Gemalto systems at the relevant time.[152] While there is some debate[153] as to the eventual success of this hacking activity, a leaked GCHQ document expresses the belief that GCHQ has had access to the entire Gemalto Network.[154] It seems indisputable that such a covert action would constitute a breach of Article 8 ECHR and potentially a breach of Article 10 ECHR also. This secretive interference with the encrypted system clearly lacked an adequate basis in law and the method of investigation was neither accessible nor foreseeable to the public.

Of course, merely making a rights-infringing law accessible and foreseeable is not sufficient in and of itself in order to ensure compliance with the Convention. Any piece of legislation mandating exceptional government access to encrypted communications must be justifiable under the Convention. Assuming that legislation is promulgated in the ordinary fashion and is sufficiently precise, there is no reason to assume it would fall foul of the legality requirements of Articles 8 and 10 ECHR. Instead, the core question is likely to lie in the necessity test. In order to be 'necessary in a democratic society', intrusions should be necessary and proportionate in the pursuit of a legitimate aim.[155] The ECtHR has stated

[151]Ronald Prins (Security expert) contended that a 'true forensic investigation in such a complex environment is not possible' in the time in which Gemalto conducted its investigation. In a similar vein, ACLU technologist, Christopher Soghoian, remarked how 'Gemalto, a company that operates in 85 countries, has figured out how to do a thorough security audit of their systems in 6 days. Remarkable'. Jeremy Scahill, 'Gemalto Doesn't Know What It Doesn't Know' *The Intercept* (25 February 2015) <https://firstlook.org/theintercept/2015/02/25/gemalto-doesnt-know-doesnt-know/> accessed 27 August; Iain Thomson, 'SIM Hack Scandal Biz Gemalto: Everything's Fine … Security Industry: No, it's really not' *The Register* (25 February 2015) <www.theregister.co.uk/2015/02/25/gemalto_everythings_fine_security_industry_hang_on_a_minute/> accessed 27 August.

[152]Simon Sharwood, 'Gemalto: NSA, GCHQ Hacked Us – but didn't Snatch Crucial SIM Keys' *The Register* (25 February 2015) <www.theregister.co.uk/2015/02/25/gemalto_spooks_popped_our_lans_not_sim_keys/> accessed 27 August.

[153]Associate Professor of Computer and Information Science at the University of Pennsylvania, Matt Blaze, described the Gemalto statements as 'surprisingly confident'. Blaze commented that '[g]etting compromised by a targeted GCHQ/NSA operation isn't negligent, but underestimating the implications of it is'. In response to Gemalto's claim that only 2G communications were at risk, Iain Thomson pointed out that Matt Green (Johns Hopkins University) has previously shown how 3G and 4G calls can also be attacked using stolen SIM keys. According to Green 'No encryption mechanism stands up to key theft, which means Gemalto is either convinced that the additional keys could not also have been stolen or they're saying that their mechanisms have some proprietary 'secret sauce' and that GCHQ, backed by the resources of NSA, could not have reverse engineered them. That's a deeply worrying statement.' Iain Thomson, 'SIM Hack Scandal Biz Gemalto: Everything's Fine … Security Industry: No, it's really not' *The Register* (25 February 2015) <www.theregister.co.uk/2015/02/25/gemalto_everythings_fine_security_industry_hang_on_a_minute/> accessed 27 August; Jeremy Scahill, 'Gemalto Doesn't Know What It Doesn't Know' *The Intercept* (25 February 2015) <https://firstlook.org/theintercept/2015/02/25/gemalto-doesnt-know-doesnt-know/> accessed 27 August; Matthew Green, 'On cellular encryption' *A Few Thoughts on Cryptographic Engineering* (14 May 2015) <blog.cryptographyengineering.com/2013/05/a-few-thoughts-on-cellular-encryption.html> accessed 27 August.

[154]____, 'CNE Access to Core Mobile Networks' (Leaked GCHQ presentation) <https://firstlook.org/theintercept/document/2015/02/19/cne-access-core-mobile-networks-2/>. accessed 27 August.

[155]In the surveillance context, sensitive issues of national interest are generally involved. This is likely to lead a wider margin of appreciation being applied by the European Court of Human Rights in any case brought before it on this issue. Regardless, the ECtHR reserves its role and has repeatedly stated that there is not an unlimited margin of appreciation and that the 'domestic margin of appreciation thus goes hand in hand with European supervision'. *Handyside v The United Kingdom* [1976] ECHR 5 [49].

that '"necessary" … implies the existence of a "pressing social need" for the interference in question[156] and the interference must be proportionate to the legitimate aim pursued'.[157] If other means of surveillance could be used to achieve the same result while causing a lesser interference, the alternative measures must be seriously considered.[158] A crucial aspect of the necessity inquiry will be the position adopted by the inquirer on the question of whether the times we live in represent a 'golden age of surveillance' or whether the intelligence available to agencies is at risk of 'going dark'.[159]

In 2011, Swire and Ahmad argued that 'the big picture for agency access to data is mostly "golden". The loss of agency access to information, due to encryption, is more than offset by surveillance gains from computing and communications technology'.[160] In light of the massive surveillance powers unveiled following the Snowden revelations, it seems even less plausible that government restrictions on encryption could meet the standards of necessity in 2015.[161] In his report on encryption, David Kaye pointed out that governments have access to a wide array of alternative surveillance tools including wiretapping, geo-location and tracking, data-mining and traditional physical surveillance.[162] Indeed, in specific reference to Apple's new encryption policy, security expert,

[156] *Dudgeon v The United Kingdom* [1981] ECHR 5 [51].

[157] Applied in the Article 8 ECHR context in *Silver v The United Kingdom* [1983] ECHR 5 [97], citing *Handyside v The United Kingdom* [1976] ECHR 5 [48]-[49].

[158] David Kaye cites the UN Human Rights Committee in order to state that a 'proportionality assessment should ensure that the restriction is "the least intrusive instrument amongst those which might achieve the desired result"'. Human Rights Committee, 'General Comment No 27 on Freedom of Movement' (1999) UN Doc CCPR/C/21/Rev.1/Add.9 [14] Human Rights Council, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye' (2015) UN Doc A/HRC/29/3, 12. When proportionality is considered by the ECtHR, however, 'it is not a scientific process'. As Christoffersen notes, the classical proportionality factors are not applied in a strict manner but are considered as weighted considerations on a scale in the context of the Convention. The classic formulation of proportionality is comprised of three sub-principles: suitability, necessity, and proportionality in the narrow sense. Jonas Christoffersen, *Fair Balance: Proportionality, Subsidiarity and Primarity in the European Convention on Human Rights* (Martinus Neijhoff, 2009); David Feldman, *Civil Liberties and Human Rights in England and Wales* (OUP, 2002) 57; David Harris and others, *Law of the European Convention on Human Rights* (Butterworths, 1995) 301; Benjamin Goold and others, *Public Protection, Proportionality, and the Search for Balance* (Ministry of Justice, 2007) ii; Robert Alexis, 'Constitutional Rights, Balancing, and Rationality' (2003) 16 *Ratio Juris* 135; Garreth Wong, 'Towards the Nutcracker Principles: Reconsidering the Objections to Proportionality' [2000] PL 92, 93. In certain circumstances, the ECtHR has adopted the least restrictive means doctrine, described by Arai-Takahashi as 'one of the most stringent forms of proportionality appraisal'. Yutaka Arai-Takahashi, *The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR* (Intersentia, 2002) 11.

[159] Peter Swire and Kenesa Ahmad '"Going Dark" Versus a "Golden Age for Surveillance"' (Center for Democracy and Technology, CDT Fellows Focus 2011) <https://cdt.org/blog/'going-dark'-versus-a-'golden-age-for-surveillance'/> accessed 27 August.

[160] Peter Swire and Kenesa Ahmad '"Going Dark" Versus a "Golden Age for Surveillance"' (Center for Democracy and Technology, CDT Fellows Focus 2011) <https://cdt.org/blog/'going-dark'-versus-a-'golden-age-for-surveillance'/> accessed 27 August.

[161] Pen America, 'Global Chilling: The Impact of Mass Surveillance on International Writers' (Results from PEN's International Survey of Writers, 2015) <www.pen.org/sites/default/files/globalchilling_2015.pdf> accessed 27 August.

[162] Human Rights Council, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye' (2015) UN Doc A/HRC/29/3, 6. See Peter Swire and Kenesa Ahmad '"Going Dark" Versus a "Golden Age for Surveillance"' (Center for Democracy and Technology, CDT Fellows Focus 2011) <https://cdt.org/blog/'going-dark'-versus-a-'golden-age-for-surveillance'/> accessed 27 August.

Jonathan Zdziarski, stated that 'eliminating the iPhone as one source I don't think is going to wreck a lot of cases'. According to Zdziarski, 'there is such a mountain of other evidence from call logs, email logs, iCloud, Gmail logs. They're tapping the whole Internet'.[163]

As government interference with encryption standards will impact everyone who uses the Internet, a high standard of necessity must be met. A difficulty in reaching this standard is posed by the fact that terrorists and organised criminals are those most likely to circumvent weak encryption.[164] Accordingly, it is questionable whether broad proposals to weaken encryption can meet the criteria of relevancy and sufficiency.[165] Kaye has pointed out that a proportionality analysis should also consider the fact that 'encroachments on encryption and anonymity will be exploited by the same criminal and terrorist networks that the limitations aim to deter'.[166] Bearing all these factors in mind, it is difficult to see how laws requiring companies to build vulnerabilities into encryption products could be compatible with the ECHR.

Compelled disclosure: the least undesirable alternative?

While there is some merit to the position that any interference with encryption standards creates unacceptable vulnerabilities in our communications systems, there is value to considering what kind of regime could allow for some limited interference with encrypted communications where it was necessary for the protection of society from crime and terrorism. While it is maintained that other measures would be preferable under a Convention analysis, one alternative scheme would require the mandatory disclosure of encryption keys. Variations of this approach are already practiced in several countries, including, somewhat infamously, in the UK where refusal to disclose a key has the potential to result in a five year prison sentence.[167]

---

[163]David Sanger and Brian Chen, 'Signaling Post-Snowden Era, New iPhone Locks Out NSA' *New York Times* (New York 26 September 2014) <www.nytimes.com/2014/09/27/technology/iphone-locks-out-the-nsa-signaling-a-post-snowden-era-.html?_r=0> accessed 27 August.

[164]Michael Chertoff, 'Cooperation and Conflict in the Relationship Between Government and Industry in Cyberspace' (Speech delivered at the Aspen Security Forum 24 July 2015) <https://www.youtube.com/watch?v=M7Ev-Wx3VT8&feature=youtu.be> accessed 27 August.

[165]It is necessary to consider whether the reasons provided by the national authorities in order to defend the interfering measure are "relevant and sufficient" under the Convention. *Handyside v The United Kingdom* [1976] ECHR 5 [50]. There is an argument that even if the ECtHR adopts a looser approach to the proportionality test that national authorities should apply the standard more rigidly. National authorities do, after all, have greater knowledge of the conditions and implications of their policies. In the surveillance context, a strict application of the proportionality test would require that the measures adopted would be 'both suitable and necessary to achieve a legitimate aim' and would strike a reasonable balance between the interests served and the interests affected. Janneke Gerards, 'The Prism of Fundamental Rights' (2012) 8 EuConst 173, 200.

[166]Human Rights Council, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye' (2015) UN Doc A/HRC/29/3, 12.

[167]Regulation of Investigatory Powers Act 2000 s 49. For an example of how this section has been used, see John Leyden, 'Computing Student Jailed After Failing to Hand Over Crypto Keys' *The Register* (8 July 2014) <www.theregister.co.uk/2014/07/08/christopher_wilson_students_refusal_to_give_up_crypto_keys_jail_sentence_ripa/> accessed 27 August. Mandatory key disclosure laws also exist and entail prison sentences where not complied with in India, France, South Africa, and Ireland. Rob Price, 'Can Police Force you to Surrender Your Password?' *The Kernel* (7 December 2014) <http://kernelmag.dailydot.com/issue-sections/features-issue-sections/11071/police-force-password-cellphone/#sthash.MjAzxQmh.dpuf> accessed 27 August; Article 19, 'Response to UN Special Rapporteur's Call for Comments on Encryption and Anonymity' (Submission February 2015) 22 <www.ohchr.org/Documents/Issues/Opinion/Communications/Article19.pdf> accessed 27 August 2015.

The model version of such a system from an ECHR perspective would require law enforcement to apply to an independent court or tribunal in order to compel the disclosure of encryption keys by the encryption key holder. The ECtHR has itself recognised that judicial control provides 'the best guarantees of independence, impartiality and a proper procedure'.[168] In cases where technology companies have excluded themselves from this knowledge – as Apple have done – it would be necessary to compel individual users to provide this information. Failure to comply would be a crime. While issues remain with this approach – particularly regarding whether such a system would constitute an interference with Article 6 ECHR[169] – it would enable some government interference with encrypted communications while circumventing the most dangerous aspects of back door access.

An additional benefit of a system of compelled disclosure (as described) is the intrinsic requirement that the individual be involved in the process.[170] This built-in trait necessitates a kind of transparency that is rare in the surveillance field. Transparency has been called the 'cornerstone' of good governance as it has an essential role to play in reducing abuse and enhancing public confidence.[171] By opening the procedure up to the targeted individual, arbitrary or unreasonable requests can be more readily challenged. Crucially, this system provides an option for government agencies and law enforcement to obtain information without making such interference the immediate automatic choice.

Conclusion

A lot of the debate concerning government restriction and sabotage of encryption has revolved around the overlapping interests of the parties involved and the fact that governments that restrict encryption expose themselves and their citizens to external threats. While these arguments have merit and are likely to be influential on government policy, they can be limiting and should not usurp consideration of the human rights implications of government actions. The reality is that the encryption debate demonstrates the polarised perspectives of the key stakeholders. As much as security experts and technology companies may attempt to convince government agencies that strong encryption is in the best interests of all parties, at this point it seems unlikely that many agencies will be swayed by the security argument alone.[172]

When considering the potential role for law and human rights in this area, it is important to recall the important role that an Appellate Court played in the eventual victory of

[168] *Klass v Germany* (1979–80) 2 EHRR 214 [67].
[169] Article 19, 'Response to UN Special Rapporteur's Call for Comments on Encryption and Anonymity' (Submission February 2015) 22 <www.ohchr.org/Documents/Issues/Opinion/Communications/Article19.pdf> accessed 27 August 2015.
[170] Article 19, 'Response to UN Special Rapporteur's Call for Comments on Encryption and Anonymity' (Submission February 2015) 22 <www.ohchr.org/Documents/Issues/Opinion/Communications/Article19.pdf> accessed 27 August 2015
[171] Laurence Lustgarten and Ian Leigh, *In from the Cold: National Security and Parliamentary Democracy* (Clarendon Press, 1994) 22. V Mäntysalo, 'The Role of Transparency and Recent Developments in Finland' (EGPA Conference, Bucharest, 2011) <http://egpa-conference2011.org/documents/PSG7/Mantysalo.pdf> accessed 27 August.
[172] Ellen Nakashima and Barton Gellman, 'As Encryption Spreads, US Grapples with Clash between Privacy, Security' *Washington Post* (Washington 10 April 2015) <https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html> accessed 27 August.

encryption in the original Crypto Wars.[173] It is contended that the ECHR could have a potential role to play in the latest battle. Based on the analysis in this article, serious questions of compatibility will have to be put to the UK government with regard to the promised legislation if it proceeds as currently planned.

As a general rule, when surveillance powers are applied in a 'blanket and indiscriminate' manner, it is difficult to strike a fair balance between the competing public and private interests.[174] The ECtHR has stated that Article 8 ECHR would be 'unacceptably weakened' if the use of modern scientific techniques in the criminal-justice system were allowed 'without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests'.[175] It seems clear that the current proposals of the UK government fail to adequately consider the privacy and expression rights of individuals who use encryption for legitimate purposes.

While a system of compelled disclosure requires a government authority to target an individual or organisation and to approach an independent tribunal with grounds justifying the intrusion, a blanket ban on encryption affects all those who wish to keep their communications secure, including those who rely on encryption in order to express and develop their political beliefs without fear of reprisal. A blanket ban will also impact innocent individuals disproportionately as criminals will be incentivised to circumvent such a ban.[176] As Phil Zimmerman has maintained for decades, '[w]hen crypto is outlawed, only outlaws will have crypto'.[177] Due to these issues and the opposition of the technology and security industry, it seems likely that the current Crypto War will end similarly to the first iteration. Equally, in spite of dour warnings, intelligence agencies will continue to develop new methods and technologies in order to investigate crime and terrorism.

Disclosure statement

No potential conflict of interest was reported by the author.

[173]Charles Mann, 'Homeland Insecurity' *The Atlantic Monthly* (Washington 28 June 2002) <www.charlesmann.org/articles/Homeland-Insecurity-Atlantic.pdf> accessed 27 August; *Bernstein v US Dep't of Justice*, 192 F 3d 1308 (9th Cir 1999), 4242.

[174]See, for example, the decision of the ECtHR in *S and Marper v The United Kingdom* [2008] ECHR 1581 [125] and the decision of the Court of Justice of the European Union in Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] WLR (D) 164 [59].

[175]*S and Marper v The United Kingdom* [2008] ECHR 1581 [112]. This case concerned blanket retention of DNA data collected from arrested individuals.

[176]Cory Doctorow, 'What David Cameron Just Proposed would Endanger Every Briton and Destroy the IT Industry' *Boing Boing* (13 January 2015) <boingboing.net/2015/01/13/what-david-cameron-just-propos.html> accessed 27 August 2015.

[177]Gordon Corera, *Intercept: The Secret History of Computers and Spies* (Weidenfeld & Nicholson, 2015) 123.