Ethics and Information Technology (2023) 25:36
https://doi.org/10.1007/s10676-023-09707-9

ORIGINAL PAPER

Specifying a principle of cryptographic justice as a response to the problem of going dark

Michael Wilson[1]

Published online: 5 July 2023

Abstract
Over the past decade, the Five Eyes Intelligence community has argued cryptosystems with end-to-end encryption (E2EE) are disrupting the acquisition and analysis of digital evidence. They have labelled this phenomenon the 'problem of going dark'. Consequently, several jurisdictions have passed 'responsible encryption' laws that limit access to E2EE. Based upon a rhetorical analysis (Cunningham in Understanding rhetoric: a guide to critical reading and argumentation, BrownWalker Press, Boca Raton, 2018) of official statements about 'going dark', it is argued there is a need for a domain-specific principle of *cryptographic justice* to reorient the debate away from competing technocratic claims about the necessity, proportionality, and accountability of digital surveillance programs. This article therefore specifies a principle of cryptographic justice by adapting more general norms of information justice to decision-making about encryption law and policy. The resulting principle is that encryption laws and policies should be designed to empower the comparatively powerless to protect themselves from domination (i.e., morally arbitrary forms of surveillance). It is argued this principle can reorient decision-making about encryption law and policy towards consideration of how cryptography impacts systems-level power dynamics within information societies.

Keywords Cryptography · Justice · Principlism · Surveillance · Rights · Privacy

Introduction

Access to cryptography is a problem of justice. This is because cryptography shapes power dynamics within information societies. Over the past decade, the Five Eyes Intelligence community has argued cryptosystems with end-to-end encryption (E2EE) are disrupting the acquisition and analysis of digital evidence (Office of Public Affairs, 2020; Five Country Ministerial, 2018; Rodenstein, 2017; Comey, 2014). They have labelled this phenomenon the 'problem of going dark' (Caproni, 2011; see also Weimann, 2016) and the associated rhetoric has been deployed to justify 'responsible encryption' laws that limit access to E2EE (see Rozenshtein, 2018; Vandenberg, 2017). In response, digital rights advocates have argued citizens have a 'right to encrypt' in pursuit of data privacy and security, freedom of expression, and protection against compelled speech (EFF, 2021; Gray, 2019; Scheurer, 1995). However, these rights-based arguments have struggled to respond to the rhetoric of going dark.

This article specifies a principle of cryptographic justice as a framework for moral decision-making about encryption laws and policies: that they should be designed to empower the comparatively powerless to protect themselves from domination (i.e., morally arbitrary forms of surveillance). It is argued this principle reorients the debate towards deliberation about the systems-level impacts of cryptography on power dynamics within information societies. This argument is developed across three sections. The first section examines the problem of going dark in detail, including examples of E2EE, recent attempts to pass 'responsible encryption' laws, and reasons for recognising an instrumental 'right to encrypt' data. Building upon this analysis, the second section examines the *rhetoric* of going dark via a rhetorical analysis (Cunningham, 2018) of statements made by officials based within FVEY jurisdictions. It is argued rhetoricians have used 'going dark' to politically justify these 'responsible encryption' laws by 'bracketing out' fundamental moral questions and focusing narrowly on competing technocratic

✉ Michael Wilson
michael.wilson@murdoch.edu.au

[1] School of Law and Criminology, Murdoch University, Perth, Australia

claims about the (un)necessity, (dis)proportionality, and (un) accountability of digital surveillance programs. The third section then specifies (i.e., Beauchamp, 2003) a principle of cryptographic justice by adapting general norms of information and data justice (Butcher, 2009; Dencik et al., 2016) to decision-making about encryption law and policy. The article then concludes by briefly applying, and critiquing the strengths and limitations of, the specified principle of cryptographic justice.

The problem of going dark

In recent years, the Five Eyes Intelligence Community (FVEY) have advocated for 'responsible encryption' laws by invoking the problem of going dark. These laws require service providers to assist law enforcement and intelligence agencies to access the contents of encrypted communications (Walden, 2018, p. 905). This section examines this policy problem in detail. The first subsection provides a brief explanation of cryptography and surveys the ongoing 'cryptographic arms race' within information societies. The second subsection focuses on implementations of E2EE and associated attempts to pass 'responsible encryption' laws. Finally, the third subsection examines the countervailing justifications for recognising a 'right to encrypt' data.

The cryptographic arms race

Understanding the debate about 'going dark' requires basic knowledge of cryptology, the "study of secret writing" (Dooley, 2018, p. 5), and more specifically, E2EE as a means of securing data-in-transit. Cryptology is constituted by two subfields: cryptography and cryptanalysis. Cryptography is the "art and science" of securing communications against access and interception by unauthorised third parties (Ferguson et al., 2010, p. 3). It is an applied form of mathematics that reorders and replaces data (Stallings, 2017; Guru & Ambhikar, 2020). Cryptanalysis is the converse process of "deciphering a message without any [or partial] knowledge of the enciphering details" (Stallings, 2017, p. 68). *Encryption* is the process of transforming plaintext into ciphertext using a *cipher* (an algorithm), while *decryption* is this process in reverse. The use of a cipher also requires a *key*—the information that tells the cipher precisely how data will be encrypted and decrypted. While a cipher is often public knowledge, keys often remain confidential. A *cryptosystem* is the broader structure within which ciphers are implemented. Finally, *End-to-end encryption* (E2EE) involves encrypting data client-side and decrypting it when it arrives at its intended destination (Ermoshina et al., 2016). Generally, this is implemented using *public key encryption* algorithms that include both *public* and *private keys* that are respectively stored server and client-side. If a cryptosystem is correctly implemented, E2EE provides the most secure method of transmitting data across a network.

Yet there is an ongoing "cryptographic arms race" within information societies insofar as wherever communications are encrypted there are efforts by adversaries to crack the corresponding ciphers (e.g., Sandywell, 2011, p. 58; Jarvis, 2021). Cryptography is not a static field as new and different ciphers are consistently being developed and improved in response to advancements in cryptanalysis. Indeed, as Singh (1999, p. 317) has argued, "every cipher has, sooner or later succumbed to cryptanalysis" and this motivates the development of new and better ciphers. This dynamic goes back to the beginnings of the field: the Vigenère cipher was developed as a secure alternative to basic substitution ciphers (Kahn, 1996, pp. 145–148). As a modern example, the Advanced Encryption Standard (AES) was developed after it became apparent that the 56-bit key length used for the Data Encryption Standard (DES) was vulnerable to, among other techniques, brute-force attacks (Diffie & Hellman, 1977; EFF, 1998). In contrast, the AES is a symmetric key algorithm that uses a key length up to a 2^{256} (Daemen & Ragmen, 2002) and is widely used for both secure disk encryption and the secure transfer of data across computer networks (Jayasinghe et al., 2014, p. 173; Heron, 2009, pp. 8–11). Recently, the Transport Layer Security (TLS) protocol was developed to ensure the security of network communications in response to vulnerabilities identified in the earlier Secure Socket Layer (SSL 3.0) protocol (CISA, 2014). In this sense, ciphers evolve in response to advancements in cryptanalysis.

Attempts to regulate encryption technologies are thus attempts to influence the dynamics of this cryptographic arms race through the instrument of law. There are various policy options available to governments seeking to regulate cryptography. These include the criminalisation of the supply, possession, or use of certain types of cryptography, placing restrictions of the export of encryption technologies, criminalising the non-disclosure of a decryption key upon provision of a lawful order or warrant, and passing 'exceptional access laws' that require 'backdoors' for law enforcement and intelligence agencies (see Walden, 2018; Koops & Kosta, 2018 for comprehensive discussion of these alternatives). Among these alternatives are also 'responsible encryption' laws that require telecommunications service providers to 'assist' law enforcement and intelligence agencies to gain access to the contents of encrypted communications (Walden, 2018, p. 905). This might involve building in a 'backdoor' into a cipher itself, inspecting client-side data before or after it is encrypted, or requiring service providers to simply avoid implementing E2EE entirely.

Indeed, even where E2EE is implemented there may remain methods of gaining access to data (e.g., Kerr & Schneier, 2017). For example, side-channel attacks target vulnerabilities in either the software or hardware used to encrypt data (Standaert, 2010; Lawson, 2009). Payload attacks can similarly be used to install remote access software on a device to enable surveillance of client communications at the points of encryption or decryption. As Kerr and Schneier (2017, p. 1008) observe, all messages "will be readable in an unencrypted form on the sender's keyboard and on the recipient's screen". This highlights the viability of alternative solutions to the problem of going dark, such as relying upon methods of lawful hacking (i.e., cryptanalysis) and covert investigations (Walden, 2018, pp. 905–906). For example, social engineering techniques can target human vulnerabilities in cybersecurity through methods of manipulation, deception, and persuasion (Krombholz et al., 2015, p. 114). Such methods can be employed by white, grey, or black hat hackers (including law enforcement) seeking to circumvent seemingly secure cryptosystems.

'Responsible encryption' laws

There has been widespread adoption of E2EE by popular communications systems, allowing billions of users to securely transmit data. For example, Meta (2023) reports that its E2EE *WhatsApp* messaging service has over 2 billion active users. *WhatsApp* is based upon the *Signal* messaging protocol, which uses a Triple Diffie-Hellman (3-DH) asymmetric key cipher involving multiple sets of public and private keys stored server and client-side (Blake-Wilson et al., 1997; Kudla & Paterson, 2005). Messages sent via *Signal* (and thus *WhatsApp*) are encrypted using these multiple key pairs, some of which will only be used one time. Similar protocols are implemented in a variety of proprietary and open-source E2EE communications systems, such as *Telegram* and *Wire*. It is the ease of access to these secure communications systems that concerns law enforcement and intelligence agencies within FVEY jurisdictions (Office of Public Affairs, 2020; Five Country Ministerial, 2018).

In response to the implementation of E2EE in these systems, the FVEY jurisdictions have pursued a range of 'responsible encryption' laws. For example, within Australia and the United Kingdom, law enforcement agencies (with judicial approval) can issue 'technical capabilities notices' to service providers requiring the development and maintenance of a 'technical capability' for intercepting and decrypting data (Telecommunications Act 1997 [Aust.], s317T; Investigatory Powers Act 2016 [UK], s253). Similarly, New Zealand police have full interception capabilities under section 9 of the *Telecommunications (Interception and Security) Act 2013* (NZ). These investigatory powers compel service providers to implement a 'man-in-the-middle' within their networks, allowing data to be intercepted, decrypted, and inspected during transit. This power does not currently exist in the United States, although there have been recent attempts to legislate similar powers via the *Compliance with Court Orders Bill 2016* (US) and *Lawful Access to Encrypted Data Bill 2020* (US). Instead, while US law enforcement can gain access to data under s103(a) of the *Communications Assistance for Law Enforcement Act 1994* (US), they cannot compel service providers to develop and maintain interception capabilities. Still, investigators have identified ways to conduct server-side surveillance via assuming direct control over messaging platforms, such as during *Operation Trojan Shield* (aka. *Operation Ironside*) where the FBI and Australian Federal Police covertly operated the messaging application *ANOM* for over 2 years (Department of Justice, 2021).

There are also ongoing debates about the scope of client-side monitoring of E2EE data. For example, under clause 110 of the proposed *Online Safety Bill 2022* (UK), the UK Office of Communications could compel service provides to use 'accredited technologies' to monitor electronic devices for unlawful content. The ambiguity of the language has prompted concerns from service providers that the legislation could mandate the use of 'client-side scanning' to monitor communications prior to being encrypted or at the point of decryption (Hern, 2023). This would add to the existing investigatory powers for client-side monitoring within FVEY jurisdictions, such as Australia's surveillance device warrants enabling the covert installation of 'data surveillance devices' on electronic devices for the purpose of monitoring data inputs and outputs (*Surveillance Devices Act 2004* [Austl.], s6). Similarly, the FBI has deployed a 'Network Investigative Technique' involving the installation of spyware on devices used by suspects during the PlayPen investigation, although the admissibility of the evidence has been challenged on the basis it was obtained illegally (Weidman, 2017, pp. 977; 995). Overall, it is clear the FVEY are pursuing a policy agenda of restricting access to E2EE via the passage of various 'responsible encryption' laws that compel server-side interception and client-side monitoring of communications.

Recognising a right to Encrypt

There is a broad coalition of privacy advocates and crypto-anarchists who oppose such efforts to restrict access to E2EE (e.g., Jarvis, 2020; Levy, 2001). As such, this subsection surveys the reasons for recognising a 'right to encrypt'. Importantly, rights are justified "not just in and of themselves, but in terms of the consequences of their existence" (Waldron, 2003, p. 208). That is, arguments for recognising the existence of a right require moral deliberation about what underlying interests it will serve. This is also true for arguments

about recognising an instrumental 'right to encrypt', which routinely draw upon four categories of interests: cybersecurity, data privacy, freedom of expression, and protection against compelled speech (e.g., Gray, 2019; Scheurer, 1995). These four categories of interests underpin most arguments advanced by the advocates of a 'right to encrypt'.

The first reason for recognising such a right is its consequences for cybersecurity. Specifically, its capacity to protect "cyberspace itself, the electronic information, the ICTs that support cyberspace, and the users of cyberspace in their personal, societal and national capacity" (von Solms & van Niekerk, 2013, p. 101). Indeed, strong or E2EE is essential for the secure transmission of data within cyberspace, while full disk encryption is the most secure method for storing data-at-rest. Cryptography has thus enabled the assimilation of ICTs into the everyday lives of citizens, allowing them to make secure phone calls, perform secure online transactions, and safely browse the web (Martin, 2020, pp. 1–2). For example, the TLS/SSL protocol is specifically designed to "prevent eavesdropping, tampering, and message forgery" by providing E2EE of data-in-transit (Turner, 2014, p. 60). It is the foundation of modern client-server communications. Furthermore, the AES-256 cipher (which is part of the TLS/SSL protocol) is essentially 'uncrackable' by modern computers (Heron, 2009, pp. 8–11; Jaysinghe et al., 2014, p. 173). In the absence of encryption like the TLS/SSL, data-in-transit would be vulnerable to unauthorised access and interception (e.g., Holtfreter & Harrington, 2015). A 'right to encrypt' thereby protects underlying interests in cybersecurity.

A second reason for recognising a 'right to encrypt' is the role of cryptography in protecting data privacy. The concept of privacy is most frequently understood as freedom from interference—a right "to be let alone" based upon a proprietary right in oneself (Warren & Brandeis, 1890, p. 205). Interests in privacy therefore include protection against the unauthorised access and interception of data. Online harassment, identity fraud, and image-based sexual abuse can constitute privacy harms independent of any material losses (e.g., Šepec, 2020). It is for this reason that cryptography is often marketed as a privacy-enhancing technology that enables individuals to control who has access to their data. For example, Phil Zimmerman (1994) named the first release of public key encryption software *Pretty Good Privacy* to reflect the privacy protective properties of the technology. Similarly, as modern examples, Telegram (2021) markets its service as "private" insofar as its "messages are heavily encrypted and can self-destruct", while Express VPN (2021) notes its service allows users to "[t]ake charge of your online privacy and security with best-in-class encryption". As such, the value of a 'right to encrypt' is linked to the dignity associated with *control* over personal information (Bloustein, 1964, p. 962), while losing control over personal information that is considered sensitive is "inherently distasteful" and harmful (Whitman, 2004, p. 1192).

A third reason for recognising a 'right to encrypt' is concerned with the consequences for freedom of expression. The 'right to encrypt' is associated with this interest in two distinct ways: (1) as preventing the chilling of lawful speech; and (2) as a form of free expression itself. The first is an extrinsic property of encryption, as it enables speech to occur free from the chilling effects of state surveillance (Dencik et al., 2016, p. 4). Researchers have observed such chilling effects impacting lawful online activity. For example, web searches for information about terrorism decreased following the Snowden disclosures, as users worried searching for phrases such as 'pipe bomb' would attract suspicion from law enforcement (Marthews & Tucker, 2015, pp. 16–25; Penney, 2015, p. 146). The use of E2EE for secure data transmission disrupts the digital surveillance capabilities that deter lawful speech. Furthermore, anonymising technologies that incorporate cryptography such as The Onion Browser (TOR) are marketed as "tools for safeguarding against mass surveillance" (Tor Project, 2021, para. 11). Indeed, privacy-enhancing technologies such as TOR are popular within jurisdictions characterised by normative commitments to individual freedoms and regions experiencing political repression (Li et al., 2013, pp. 1272–1273; Jardine, 2018, pp. 448–449). A 'right to encrypt' thus has value as it enables free expression outside the control of the state.

A related argument is that encrypted speech is, itself, a form of free expression. Dulay (2019, p. 131) has described this as a "right to speak in code" as encrypted speech is simply speech that is not comprehensible to a third party. During the 'crypto war' of the 1990s, Jill Ryan (1996, p. 1201) similarly described this aspect of the 'right to encrypt' as the "freedom to speak unintelligibly". From this perspective, encrypted speech is considered morally equivalent to speaking with another person using a language that a third party to the conversation cannot understand. Infringing on a 'right to encrypt' would be like coercing a person to not speak in a particular language. However, this line-of-reasoning can be challenged by distinguishing between speech and conduct. The process of encrypting (or translating) speech using computer code might be classified as 'conduct' as it requires an action. Indeed, Collins (1997, p. 2691) has criticised any "right to speak in cryptographic computer code" as a misunderstanding of the 'act' of encryption insofar as it is a form of conduct rather than speech. If this is the case, the process of encryption would fall within the scope of legitimate regulation without interfering with free expression (Petersen, 2015, p. 415).

A fourth reason for recognising a 'right to encrypt' is protection against compelled speech by the state. Specifically, interfering with a 'right to encrypt' by compelling disclosure of a cryptographic key has been argued to interfere with

the common law privilege against self-incrimination (Daly, 2014, p. 59). This argument hinges on whether the disclosure of a cryptographic key is considered a form of testimonial or non-testimonial evidence (e.g., McAdow, 1966). Generally, non-testimonial evidence can be lawfully acquired during criminal investigations without the consent of a suspect. An analogous example is a production order that compels access to premises under the authority of a warrant, including requirements to grant access to a locked filing cabinet filled with documentary evidence. This is the approach adopted by most common law jurisdictions (Hochstrasser, 2021). However, there is disagreement about whether the 'act' of disclosing a cryptographic key is "implied testimony that the suspect is familiar with the contents of the device" (Adam & Barns, 2020, p. 224; Kerr, 2019). From this perspective, compelling an individual to disclose a cryptographic key may be morally equivalent to compelling implied testimony against themselves. As such, a "right to remain encrypted" (Soares, 2012, p. 2001) might be derived on the basis that disclosure of a cryptographic key is compelled acknowledgement of the contents of an encrypted device.

The rhetoric of going dark

The recent success of the rhetoric of going dark is partially attributable to the technocratic character of contemporary rights-based discourse. That is, there is a tendency for debates about 'going dark' and the 'right to encrypt' to descend into competing claims about the (un)necessity, (dis)proportionality, and (un)accountability of digital surveillance programs. This section thus explores the rhetoric of going dark via a rhetorical analysis (Cunningham, 2018) of the language used to justify 'responsible encryption' laws and the corresponding limitations of technocratic language as an argumentative strategy for justifying a 'right to encrypt'. Drawing upon Jeremy Waldron's (1989, 2003) work on rights in conflict, it will be argued the rhetoric of going dark invariably narrows the scope of a 'right to encrypt' using technocratic principles of necessity, proportionality, and accountability. As such, the first subsection will examine how the rhetoric of going dark is used to 'bracket out' fundamental moral questions from the debate, while the second subsection will examine how the rhetoric of going dark narrows the scope of an instrumental 'right to encrypt' using these technocratic discourses.

Justifying 'responsible encryption' laws

One key feature of the rhetoric used to justify 'responsible encryption' laws is a focus on empirical claims rather than normative issues. In this sense, the rhetoric of going dark 'brackets out' moral discourse from historical and contemporary policy debates about E2EE. The first contemporary attempt within the FVEY to regulate E2EE by invoking a precursor to the rhetoric of going dark came within the US *Comprehensive Counter-Terrorism Bill* (1991) and associated efforts at implementing backdoors into telecommunications (i.e., Key Escrow). For example, Section 2201 of the *Comprehensive Counter-Terrorism Bill* (1991) included a non-binding resolution expressing a view that:

> [P]roviders of electronic communications services and manufacturers of electronic communications service equipment shall ensure that communications systems permit the government to obtain the plain text contents of voice, data, and other communications when appropriately authorized by law.

While the Bill was ultimately withdrawn, it was soon followed by the US Government's Clipper Chip initiative. This initiative involved implementing escrowed keys into American telephones by installing a chip with a symmetric key cipher called *Skipjack*. Copies of the cryptographic keys stored by the government would be available to law enforcement upon issue of a judicial warrant (Pednekar-Magal & Shields, 2003, p. 443). Once again, the US Government's argument was a precursor to the rhetoric of going dark. For example, the White House (1994, para. 2) explained the rationale for key escrow in the following terms:

> Advanced encryption technology offers individuals and businesses an inexpensive and easy way to encode data and telephone conversations. Unfortunately, the same encryption technology that can help Americans protect business secrets and personal privacy can also be used by terrorists, drug dealers, and other criminals.

The implementation of key escrow would therefore "provide Americans with secure telecommunications without compromising the ability of law enforcement agencies to carry out legally authorized wiretaps" (The White House, 1994, para. 4). This framing narrowly focuses on the empirical utility of key escrow as a policy solution. Ultimately, through a coalition of digital rights advocacy and corporate interests in secure e-commerce (Levy, 2001, pp. 305–311), various efforts at weakening E2EE during the 1990s failed.

Following the September 11, 2001 attacks, the US Government significantly expanded the digital surveillance capabilities of law enforcement and intelligence agencies. Consequently, debates about encryption law and policy mostly disappeared from the public sphere as the FVEY focused on covert methods of digital surveillance. For example, Project BULLRUN was an NSA operation involving multiple strategies for cracking encryption, including the intentional weakening of cryptographic standards, pursuing developments in cryptanalysis without public disclosure, and forming covert agreements with technology companies to enable access to

data (Yoo, 2014, p. 34). It has been reported the NSA pushed for the standardisation of a flawed pseudorandom number generator for use in cryptosystems known as the Dual EC Standard (Dual_EC_DRBG) as part of BULLRUN (Bernstein et al., 2016; Menn, 2013, para. 2). During this period the 'arms race' was more covert—taking place behind the scenes. This was aided by assertions that digital surveillance capabilities needed to remain secret to protect national security (Masco, 2010, p. 448).

Yet the rhetoric of going dark re-emerged within public debates about encryption law and policy in the post-Snowden era. Use of the rhetoric thus reflected a renewed commitment by the FVEY to justify restrictions on E2EE. Specifically, the phrase 'going dark' was introduced into the encryption policy lexicon during an appearance before the US House Judiciary Committee by FBI General Counsel Caproni (2011, para. 4), where she described a "capabilities gap" between the state's lawful authority and technical abilities:

> We call this capabilities gap the "Going Dark" problem. As the gap between authority and capability widens, the government is increasingly unable to collect valuable evidence in cases ranging from child exploitation and pornography to organized crime and drug trafficking to terrorism and espionage—evidence that a court has authorized the government to collect. This gap poses a growing threat to public safety.

By focusing narrowly on the 'lawfulness' of the authority to intercept communications, Caproni (2011) sidesteps questions about the ethics of digital surveillance. Instead, she presumes the state ought to have such authority. Similarly, in the aftermath of the 2015 San Bernardino attack, the FBI argued Apple needed to assist with providing access to the contents of a perpetrator's mobile phone due to the mere existence of a warrant (Bay, 2017). Thereby, the FBI employed a rhetorical device known as a *metonym* to subsume moral concerns about data access into the fact that a legal 'warrant' had been issued (Lauer & Lauer, 2018, p. 54).

Appeals to the problem of going dark has thus become the dominant rhetorical strategy deployed by the FVEY for justifying 'responsible encryption' laws over the past decade. For example, in an address to the Brookings Institute, FBI Director Comey (2014, paras. 11, 32 and 59) made the following remarks about access to encrypted communications:

> Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority. We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so… We aren't seeking a back-door approach. We want to use the front door, with clarity and transparency, and with clear guidance provided by law. We are completely comfortable with court orders and legal process—front doors that provide the evidence and information we need to investigate crime and prevent terrorist attacks… We need assistance and cooperation from companies to comply with lawful court orders, so that criminals around the world cannot seek safe haven for lawless conduct.

Again, this rhetoric avoids addressing underlying questions about whether citizens *ought* to be able to render their communications inaccessible to the state. A presumption that the state has moral authority to access data is articulated using metonyms of 'lawfulness', 'warrants', and 'front doors'. Indeed, public officials have argued they are simply introducing the 'rule of law' into otherwise 'lawless spaces', 'law-free zones', and 'hiding places' (Hewson & Harrison, 2021, pp. 11, 12). Furthermore, the audience is directed to focus on the 'needs' of law enforcement and the reasonableness of 'assistance and cooperation' from service providers. As such, fundamental ethical questions are 'bracketed out' and replaced by technocratic claims about the necessity and proportionality of 'responsible encryption' laws mandating access to plaintext copies of encrypted communications (see also Rodenstein, 2017, paras. 50–52). This strategy of narrowly focusing on empirical questions is particularly evident in the argumentative discourse between privacy advocates and law enforcement officials.

Narrowing the right to encrypt

There are persuasive reasons for recognising an instrumental 'right to encrypt'. However, rights are never absolute, and conflicts must be resolved through the application of moral principles (Waldron, 1989, 2003). It may be useful to first consider this problem in abstract terms. Within a community, *Alice* might be considered 'free' insofar as she is not interfered with by *Bob*. Thus, to protect *Alice*'s right to non-interference, *Bob* must be prevented from interfering. Some degree of interference with *Bob*'s freedom is thus required to protect *Alice*'s freedom. In this sense, interferences with freedoms are built into the basic logic of rights. Furthermore, such logics justify pre-emptive interferences with freedoms (e.g., see Ashworth and Zedner, 2014). For example, to prevent *Bob* interfering with *Alice*, access to the 'instruments of interference' (such as E2EE) might need to be regulated by the state. This can thus limit *Carol*'s right to access such instruments. Thus, resolving conflicts of rights, and thereby defining their scope, requires the elucidation of moral principles.

The rhetoric of going dark excels at narrowing the 'right to encrypt' using a façade of technocratic precision by applying principles of *necessity*, *proportionality*, and *accountability* (see Mann et al., 2018, p. 378). Indeed, such principles are used to 'trade-off' interests in ways that favour the advocates of digital surveillance programs (Bronitt & Stellios, 2005, p. 887; Barnard-Wills, 2011, p. 555; Suzor et al., 2017, p. 3). Competing claims about the (un)necessity and (dis)proportionality of digital surveillance go to questions about their capacity to achieve desired outcomes, the reasonableness of an interference, and the viability of less intrusive policy options (Macnish, 2018, pp. 145, 151), while claims about (un)accountability concern what social and legal structures provide sufficiently independent oversight of decisions about, and the exercise of, digital surveillance powers (Mann et al., 2018, pp. 378, 379). Yet it is the malleability of such principles that render them vulnerable to distortion in rhetorical justifications for 'responsible encryption' laws.

The first requirement for satisfying the necessity principle is that there is, indeed, a policy problem that requires state intervention. Few scholars contest that cryptography is misused by criminals. Indeed, offenders have been observed to consciously use encryption to evade detection by law enforcement and intelligence agencies (van der Bruggen & Blokland, 2021, p. 960; Jardine, 2021, p. 13; Kowalski et al., 2019, p. 248; Hutchings and Holt, 2015, p. 600). While the specific offences vary in severity, this includes harms such as the distribution of child exploitation material (O'Brien, 2014, pp. 247, 248; Maras, 2014, p. 22) and the sale of illegal drugs and weapons (Phelps & Watt, 2014, pp. 266, 267; Martin, 2014, p. 358). For example, a semantic analysis of indexed webpages on the dark web (n = 1171) suggests at least 18% of darknet sites are being used for distributing child exploitation material (Guitton, 2013, p. 2809). Similar research using an automated web crawler suggests 10–15% of darknet pages distribute such material (Spitters et al., 2014, p. 223). Further, an analysis of the *Silk Road 2.0* marketplace suggests illicit substances constituted 19% of all advertised products (Dolliver, 2015, p. 1119). Thus, it is easy to satisfy the first requirement of the necessity principle.

Yet despite these criminal misuses of cryptography, the critics of 'responsible encryption' laws argue they are still not necessary. That is, the necessity principle is not satisfied if there are alternative solutions available (e.g., Swire and Ahmad, 2012, p. 420). This claim suggests law enforcement have (more than) enough access to information for the purposes of criminal investigations. For example, the American Civil Liberties Union (2015, para. 9) has argued that "encryption is not a problem to be solved" on the basis that:

> [L]aw-enforcement authorities are now operating in a "golden age of surveillance." While technology promises to secure the content of our communications, it has at the same time made our lives more transparent to law enforcement than ever before. With little effort, police forces can now determine a suspect's exact location over a period of months, his every confederate, and every other digital fingerprint he leaves when interacting with technology.

As such, it is claimed the investigative capabilities of law enforcement have not been unduly disrupted by cryptography (e.g., Walden, 2018; Koops and Kosta, 2018). Alternative investigatory options include undercover operations, the use of cryptanalysis to target vulnerabilities in the implementation of cryptosystems, metadata surveillance capabilities, and open-source intelligence gathering (Walden, 2018, pp. 905, 906). Indeed, one analysis of Dutch court cases between 2015 and 2019 (n = 3214) suggests, of those cases that proceed to trial, "law enforcement appears to be as successful in prosecuting offenders who rely on encrypted communication as those who do not" (Hartel & van Wegberg, 2021, p. 1).

However, the necessity principle remains malleable to distortion by the rhetoricians of going dark. These advocates of 'responsible encryption' laws merely assert such powers are necessary by focusing on the impacts on *investigations* rather than prosecutions. For example, former FBI director Wray (2017, para. 36) noted that "in the first 11 months of this fiscal year alone, we were unable to access the content of more than 6900 mobile devices using appropriate and available tools, even though we had the legal authority to do so". Similarly, the Australian Department of Home Affairs (2018, p. 5) has argued that over 90% of the Australian Security Intelligence Organisation's priority investigations are disrupted by encryption. This data is drawn from law enforcement agencies themselves, rendering it difficult for digital rights advocates to contest. The claim is reiterated by the rhetoricians of going dark, who deploy the necessity principle to narrow the scope of any 'right to encrypt'.

The proportionality principle is similarly deployed to both justify and criticise the reasonableness of 'responsible encryption' laws. For example, cybersecurity experts have warned that weakening cryptosystems will "open doors through which criminals and malicious nation-states can attack the very individuals law enforcement seek to defend" (Abelson et al., 2015, pp. 24, 25). Thus, they argue 'responsible encryption' (and exceptional access) laws will lead to greater costs than their purported benefits. Therein, even if such powers are necessary to prevent the criminal misuses of cryptography, the detrimental consequences for cybersecurity interests undermine the state's claims about proportionality. Yet the rhetoricians of going dark simply

focus on different categories of harm to satisfy the proportionality principle and justify 'responsible encryption' laws. For example, the top law enforcement officials in the FVEY (Office of Public Affairs, 2020, paras. 2, 3) have argued:

> Particular implementations of encryption technology, however, pose significant challenges to public safety, including to highly vulnerable members of our societies like sexually exploited children… We call on technology companies to work with governments to… [e]nable law enforcement access to content in a readable and usable format where an authorisation is lawfully issued, is necessary and proportionate, and is subject to strong safeguards and oversight.

The proportionality principle is here deployed to assert that harms to "sexually exploited children" are severe enough to warrant "law enforcement access to content in a readable and usable format". This strategy of framing the issue as about selective types of harm is well-documented as appealing to the "horsemen of the infopocalypse" (Jordan, 2015, pp. 104, 105; Carey and Burkell, 2007). As such, the rhetoricians of going dark focus on selective harms, ignoring concerns about cybersecurity vulnerabilities if access to E2EE is restricted.

This rhetorical strategy is possible because of the fluidity of 'harm' as a moral signifier. Indeed, counterarguments that digital surveillance programs are *dis*proportionate rely upon competing claims that the 'harms' occurring in cyberspace are being exaggerated (Yar & Steinmetz, 2019, pp. 97; 210–213). For example, technologist Schneier (2019, paras. 2, 7) has argued regulators are "scaring people into supporting backdoors":

> Since the terrorist attacks of 9/11, the US government has been pushing the terrorist scare story. Recently, it seems to have switched to pedophiles and child exploitation… None of us who favor strong encryption is saying that child exploitation isn't a serious crime, or a worldwide problem. We're not saying that about kidnapping, international drug cartels, money laundering, or terrorism. We are saying three things. One, that strong encryption is necessary for personal and national security. Two, that weakening encryption does more harm than good. And three, law enforcement has other avenues for criminal investigation than eavesdropping on communications and stored devices.

These types of claims that "weakening encryption does more harm than good" similarly assume there are objective measures of 'harm' that can inform assessments of proportionality. Yet the severity of a 'harm' is not only about the quantity of events. It is also linked to intersubjective judgements about the moral gravity of an action. Indeed, Cohen (2002, p.xxxiv), the theorist of moral panics, has observed, "we have neither the quantitative, objective criteria to claim that R (the reaction) is 'disproportionate' to A (the action) nor the universal moral criteria to judge that R is an 'inappropriate' response to the moral gravity of A". As such, given how cryptography can be misused by criminals, the proportionality principle is readily distorted by rhetoricians to narrow the scope of a 'right to encrypt'.

The proportionality principle is also malleable due to the connections rhetoricians draw between 'harm' and the 'risk' of harm. As Ashworth and Zedner (2014, p. 95) have argued, "[i]f a certain form of wrongdoing is judged serious enough to criminalize, it ought surely to follow that the state… should assume responsibility for taking steps to protect people from such wrongdoing and harm". This is the logic of preventive justice, where "the possibility of forestalling risks competes with and even takes precedence over responding to wrongs done" (Zedner, 2007, p. 262). Indeed, interviews with cybersecurity experts highlight how concerns about 'harm' are predominantly based upon hypothetical, rather than actual, scenarios (Carroll & Windle, 2018, p. 285). For example, former FBI director Comey (2014, paras. 11, 32) made the following observation about the protective and preventive functions of law enforcement access to encrypted communications:

> We call it "Going Dark," and what it means is this: Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority… We are completely comfortable with court orders and legal process—front doors that provide the evidence and information we need to investigate crime and prevent terrorist attacks.

These protective and preventive functions of digital surveillance programs are thereby invoked within the rhetoric of going dark to further shift the 'balance' in assessing proportionality. Consequently, competing claims about the *dis*proportionality of 'responsible encryption' laws are readily neutralised by invoking the risks of cybercrime and terrorism.

One final aspect of the rhetoric of going dark used to narrow the scope of the 'right to encrypt' is the principle of *accountability*. Such rhetoric invokes the 'objective' and 'neutral' role of the judiciary or subject-matter experts as arbiters of striking the right 'balance' between competing interests. However, such 'safeguards' are also readily deployed in pursuit of digital surveillance programs (Mann et al., 2018, p. 378). For example, one Five Country Ministerial Communique (2018, paras. 25–26) included the following comments:

> Each of the Five Eyes jurisdictions will consider how best to implement the principles of this statement,

> including with the voluntary cooperation of industry partners. Any response, be it legislative or otherwise, will adhere to requirements for proper authorization and oversight, and to the traditional requirements that access to information is underpinned by warrant or other legal process.

The rhetoricians of 'going dark' thus employ the accountability principle ('authorization and oversight') as a strategy for negating concerns about the scope of 'responsible encryption' laws. In this sense, the requirement to obtain a 'warrant' is framed as sufficient for satisfying the principle (e.g., Lauer and Lauer, 2018). There is no consideration that such powers might require democratic or individual models of consent, and instead faith is placed in judicial and technical experts as sources of non-arbitrary power. This highlights the limitations of existing arguments for a 'right to encrypt' insofar as they rely upon the same technocratic principles as the advocates of 'responsible encryption' laws. Consequently, rhetoricians are able to narrow the scope of such a right via the malleability of necessity, proportionality, and accountability.

The principle of cryptographic justice

Resolving conflicts between rights invariably requires the 'balancing' of the underlying interests they serve (Waldron, 2003; Raz, 1986). Moral principles can thus help to guide decisions about how such conflicts ought to be resolved. As noted, the advocates of a 'right to encrypt' and the rhetoricians of 'going dark' similarly focus on technocratic claims about the (un)necessity, (dis)proportionality, and (un) accountability of digital surveillance programs. These types of technocratic principles attempt to 'balance' interests using utilitarian standards and the pretence of scientific precision. Yet their rhetorical malleability allows those with social and political power to influence the outcomes of their application. This highlights the need for a domain-specific principle of justice to guide moral deliberation about the impacts of cryptography on power dynamics within information societies. Such a principle can highlight the value of a 'right to encrypt' without relying on technocratic language.

The process of *specification* involves identifying domain-specific moral principles for decision-making, including within technology and cybersecurity ethics (e.g., Formosa et al., 2021, p. 3). It involves "reducing the indeterminateness of general norms to give them increasing action guiding capacity, while retaining the moral commitments to the original norm" (Beever & Brightman, 2016, p. 282, summarising Beauchamp, 2003). Indeed, for a moral principle to be useful for decision-making, it should ideally be specified to a particular domain (Beauchamp & DeGrazia, 2004, p. 61). A principle of cryptographic justice should therefore be specified with reference to existing scholarship about data and information justice (e.g., Butcher, 2009; Johnson, 2014; Dencik et al., 2016) and broader literature about the moral characteristics of cryptography and surveillance (e.g., Beltramini, 2021; Rogaway, 2015). These literatures can provide the basis for a domain-specific principle of cryptographic justice.

Existing norms and moral characteristics

The concepts of information justice and data justice provide ideal foundations as they already adapt the broader concept of *justice* to the context of information societies. Broadly, information societies are where "economic relations are no longer primarily organized on the basis of material goods… everything is organized on the basis of information and knowledge" (Lyon, 2013, p. 1). It is within this context that the notions of information and data justice have been developed. For example, the concept of 'information justice' describes how socio-economic inequities are being exacerbated by the integration of ICTs within most facets of the economy, thereby "conferring power disproportionately on the information-wealthy at great expense to the information-poor" (Butcher, 2009, p. 57; Johnson, 2014). This concept was further developed by Dencik et al. (2016, p. 9) as 'data justice' to articulate how the commodification of personal information "requires us to scrutinise the interests and power relations at play in 'datafied' societies that enfranchise some and disenfranchise others". Broadly, data justice is thus about "fairness in the way people are made visible, represented and treated as a result of their production of digital data" (Taylor, 2017, p. 10).

Access to data is thus a problem of justice as it influences power dynamics within information societies. As such, the concepts of information and data justice have been deployed to critique the ethics of data collection regimes (Dencik et al., 2016). For example, scholars have examined how the datafication of community transport services using information from cellular phones has led to the invisibility of elderly populations in policy-making processes (Sourbati & Behrendt, 2021), how government practices of verifying the identities of displaced persons impact patterns of urban planning policymaking that disadvantage them (Heeks & Shekhar, 2019), how the datafication and automation of welfare programs has accelerated the surveillance of impoverished populations (Mann, 2020), and how transparency laws governing fossil fuel industries can enhance citizen oversight and regulation (Jalbert et al., 2019). In each of these scenarios, scholars have critiqued how access to information variously (dis)empowers individuals, corporations, and the state.

Cryptography further complicates these types of problems because it enhances *control* over who has access to this information. Indeed, as Rogaway (2015, p. 42) has argued, cryptography "can be developed in directions that tend to benefit the weak or the powerful" and this requires moral deliberation about both its character and consequences. In this sense, there are unique issues associated with encryption law and policy that require further specification and consideration. Here, it is useful to engage with the broader literature about the underlying moral characteristics of cryptography. One view among 'crypto anarchists' is that cryptography is, itself, morally neutral. That it is merely a tool that may be (mis)used by human decision-makers. This worldview is succinctly expressed by crypto anarchist Timothy C. May (quoted in Moore and Rid, 2016, pp. 24, 25) within the phrase "crypto = guns", where he draws a moral equivalence between access to cryptography and the right to keep and bear arms. It is consistent with the value-neutrality thesis (Pitt, 2014), which asserts that technical artifacts do not contain intrinsic normative characteristics. Indeed, a content analysis of the hacker publication *2600: The Hacker Quarterly* between 2002 and 2012 reveals how 'individual responsibility' is the central rhetorical device used by computer hackers to oppose state regulation of technology, regardless of any harmful consequences (Steinmetz & Geber, 2015, pp. 37–42). This is a line-of-reasoning that informs techno-libertarianism and thus reflects one model of justice (i.e., Nozick, 1974) that a principle could be based upon.

However, not all 'crypto anarchists' subscribe to a form of radical individualism, place faith in free markets, or subscribe to meritocracy as a model for a just society. There is diversity of thought within the movement and this is reflected in the descriptions of cryptography as a "surprisingly political" (Zimmerman, 1994, para. 4) or "inherently political tool" (Rogaway, 2015, p. 1). In this sense, the moral character of cryptography is intrinsically linked to how it "rearranges power" based upon who can (and cannot) secure their data (Rogaway, 2015, p. 1). In contrast to the value-neutrality thesis, moral values are therefore built into cryptographic artefacts by virtue of their purpose (or *telos*) within an information society (see Miller, 2021). In this vein, crypto anarchists intuitively understand cryptography as a technology for resisting domination – the arbitrary exercise of surveillance powers (Beltramini, 2021, p. 102; Kinna and Prichard, 2019). This prompts the development and dissemination of new and better ciphers for the purpose (*or telos*) *of* resisting arbitrary state and corporate surveillance. For example, David Chaum's (1985, p. 1030) foundational paper on cryptocurrencies argued for their revolutionary potential to "make big brother obsolete" by empowering citizens to circumvent centralised financial institutions, Phil Zimmerman's (1994) release of *Pretty Good Privacy* empowered ordinary citizens to use public key cryptography to avoid state surveillance programs, and WikiLeaks' use of cryptography as a "technology of dissent" enables whistleblowing about state crimes (Curran & Gibson, 2013, p. 307). Far from a form of techno-libertarian praxis, such 'anti-surveillance' technologies are often developed collaboratively and released as Free and Open-Source Software in pursuit of the common good (Taffel, 2015; Rogaway, 2015). It is in this sense that a principle of cryptographic justice should acknowledge the purpose (or *telos*) of cryptography as about empowering the comparatively powerless.

This is consistent with recent scholarship in surveillance ethics that argues a civic republican model of 'non-domination' is useful for conceptualising when interferences with privacy are morally arbitrary. From this perspective, arbitrary interferences with privacy are those that have not been authorised via meaningful democratic decision-making processes (Newell, 2014, p. 520). For example, Newell (2014, p. 520) has argued that even benevolent surveillance programs are akin to benevolent dictators who retains the potential to dominate citizens in the absence of democratic checks and balances. This metaphor of the 'friendly despot' is a useful device for conceptualising liberty as being about non-domination, as a 'friendly despot' may change their mind and arbitrarily interfere at any point in the future (Pettit, 2011, p. 714). From this perspective, depriving the subjects of surveillance the opportunity to participate in self-government via paternalistic 'responsible encryption' laws is an act of domination regardless of the intentions of lawmakers. Given concerns about the tendency of FVEY officials to engage in a politics of fear and 'policy laundering' to legitimate surveillance powers (Ogasawara, 2022; Simone, 2009), it is argued a moral language of 'non-domination' better captures the concerns of digital rights advocates with regards to how access to E2EE influences power dynamics within information societies.

Specifying the principle of cryptographic justice

Building upon these literatures, the principle of cryptographic justice can be specified in the following way: the design of encryption laws and policies should empower the comparatively powerless to protect themselves from domination (i.e., arbitrary surveillance). This acknowledges the inherently moral character of cryptography as impacting power dynamics within information societies and not merely as a tool that is (mis)used by individuals. As such, the principle of cryptographic justice can guide more robust decision-making about the morality of alternative options for encryption law and policymaking.

For example, a decision to implement 'responsible encryption' laws will have the consequence of empowering eavesdroppers to intercept encrypted communications.

Indeed, undermining the availability of encryption technologies will invariably expose ordinary users to man-in-the-middle attacks and other data breaches orchestrated by malicious third parties. Potential eavesdroppers include state and non-state actors with high levels of digital literacy, and they are therefore *powerful* agents within an information society. While it is true that virtuous eavesdroppers might protect the comparatively powerless, 'responsible encryption' laws will always have the effect of further *disempowering* the comparatively powerless—the ordinary users who lack knowledge of information security. In this sense, 'responsible encryption' laws cannot satisfy a principle of cryptographic justice as they further empower the already powerful. Alternatively, relying and expanding upon existing methods of cryptanalysis, undercover network operations, and criminalising non-compliance with production orders for documentary evidence, all serve the interests of victims while not systemically weakening the data privacy and security of ordinary users. Overall, a domain-specific principle of cryptographic justice can enable a systems-level critique of how encryption laws and policies (dis)empower moral agents to protect themselves.

A moral principle that embraces an orientation towards the interests of the comparatively powerless addresses some (but not all) of the limitations identified with the technocratic language used to justify and narrow the 'right to encrypt'. Indeed, the supposed neutrality of 'balancing' using principles of necessity, proportionality, and accountability lends itself to reinforcing and exacerbating existing power dynamics within information societies, as those already with power can shape the outcomes of debates within the public sphere. As noted above, the rhetoricians of going dark effectively distort the concepts of harm, risk, and reasonableness to influence judgements about the necessity, proportionality, and accountability of alternative encryption laws and policies. By way of contrast, a principle of cryptographic justice that explicitly adopts an orientation towards the interests of the comparatively powerless does not pretend to neutrality or objectivity in moral decision-making. Rather, by asserting the moral priority of empowering the comparatively powerless, rather than the interests of the state (and its agents) to paternalistically protect them, the moral calculus shifts more clearly in favour of justifying the 'right to encrypt' and encouraging law enforcement to adopt alternative investigative strategies for responding to the problem of going dark.

Yet this is not a silver bullet for those who wish to argue for an absolute 'right to encrypt' or dismiss the problem of going dark. Even where the interests of the comparatively powerless are morally prioritised there remains tension and conflicts. Two key issues concern the need to develop shared and unambiguous definitions of *who* constitutes the 'comparatively powerless' and *what* constitutes 'non-arbitrary' sources of power. Without some measure of agreement, a principle of cryptographic justice will be similarly vulnerable to rhetorical distortion. This will require further research beyond the scope of the present article. Further, the data privacy and security of ordinary users will always conflict with the interests of cybercrime victims. Indeed, cryptography does empower malicious actors to engage in harmful activities and undermines the potential for victims to restore material and non-material losses. However, despite these limitations, a principle of cryptographic justice has one significant benefit: it requires decision-makers to consider the broader social and political impacts of cryptography, rather than focusing exclusively on the actions of individuals. It is thus useful for highlighting the benefits of E2EE for ordinary users, including data privacy and security, protecting freedom of expression, and protection against compelled speech. It acknowledges that in adjudicating conflicts there can be no 'scientific' balancing of interests. As such, the principle of cryptographic justice reorients the debate away from any pretence of technocratic objectivity and towards a systems-level analysis of power relations. It can thus assist decision-makers to avoid reinforcing unjust power dynamics by, for example, granting the state increasingly invasive access to the data of ordinary citizens. In this sense, a principle of cryptographic justice serves to complement and contextualise the application of other principles—such as necessity, proportionality, and accountability—rather than replace them.

Conclusion

Access to cryptography is a problem of justice within information societies as it shapes who has access to what information. Yet despite the efforts of digital rights advocates to articulate the value of a 'right to encrypt', multiple jurisdictions within the FVEY have recently passed 'responsible encryption' laws that restrict access to E2EE. As such, this article has specified a principle of cryptographic justice as a response to the problem of going dark: encryption laws and policies should be designed to empower the comparatively powerless to protect themselves from domination (i.e., arbitrary surveillance). This principle helps to reorient the debate towards systems-level analyses of power within information societies. Such a principle is therefore useful for addressing some (but not all) of the limitations associated with the language used to justify a 'right to encrypt'. Indeed, there are good reasons for recognising such a right, including users' data privacy and security, protecting freedom of expression within cyberspace, and protection against compelled speech by the state. However, the rhetoricians of the problem of going dark have successfully narrowed the scope

of any such right by appealing to technocratic principles of necessity, proportionality, and accountability. It is argued this rhetoric is more effectively responded to by avoiding any pretence of technocratic 'neutrality' or 'objectivity' in moral decision-making, and instead by invoking an explicit orientation towards the *telos* of cryptography as empowering the comparatively powerless to resist morally arbitrary forms of surveillance.

Funding Open Access funding enabled and organized by CAUL and its Member Institutions.

References

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., "Whit," Gilmore, J., Green, M., Landau, S., Neumann, P. G., Rivest, R. L., Schiller, J. I., Schneier, B., Specter, M. A., & Weitzner, D. J. (2015). Keys under doormats. *Communications of the ACM*, *58*(10), 24–26. https://doi.org/10.1145/2814825.

Adam, L., & Barns, G. (2020). Digital strip searches in Australia: A threat to the privilege against self-incrimination. *Alternative Law Journal*, *45*(3), 222–227. https://doi.org/10.1177/1037969X20923073.

American Civil Liberties Union (2015). Encryption is not a problem to be solved, but a crucial tool for freedom and security. https://www.aclu.org/blog/free-future/aclu-un-encryption-not-problem-be-solved-crucial-tool-freedom-and-security.

Ashworth, A., & Zedner, L. (2014). *Preventive justice*. Oxford University Press.

Australian Department of Home Affairs (2018). *Submission to Parliamentary Inquiry into the Telecommunicatons and Other legislation (Assistance and Access) Bill 2018*. https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/TelcoAmendmentBill2018/Submissions

Barnard-Wills, D. (2011). UK news media discourses of surveillance. *The Sociological Quarterly*, *52*(4), 548–567. https://doi.org/10.1111/j.1533-8525.2011.01219.x.

Bay, M. (2017). The ethics of unbreakable encryption: Rawlsian privacy and the San Bernardino iPhone. *First Monday*. https://doi.org/10.5210/fm.v22i2.7006.

Beauchamp, T. L. (2003). Methods and principles in biomedical ethics. *Journal of Medical Ethics*, *29*(5), 269–274.

Beauchamp, T. L., & DeGrazia, D. (2004). Principles and Principlism. In G. Khushf (Ed.), *Handbook of Bioethics: Taking Stock of the Field from a Philosophical Perspective* (pp. 55–74). Springer. https://doi.org/10.1007/1-4020-2127-5_3

Beever, J., & Brightman, A. O. (2016). Reflexive principlism as an Effective Approach for developing ethical reasoning in Engineering. *Science and Engineering Ethics*, *22*(1), 275–291. https://doi.org/10.1007/s11948-015-9633-5.

Beltramini, E. (2021). Against technocratic authoritarianism. A short intellectual history of the cypherpunk movement. *Internet Histories*, *5*(2), 101–118. https://doi.org/10.1080/24701475.2020.1731249.

Bernstein, D. J., Lange, T., & Niederhagen, R. (2016). Dual EC: A Standardized Back Door. In P. Y. A. Ryan, D. Naccache, & J.-J. Quisquater (Eds.), *The New Codebreakers* (pp. 256–281). Springer. https://doi.org/10.1007/978-3-662-49301-4_17

Blake-Wilson, S., Johnson, D., & Menezes, A. (1997). Key agreement protocols and their security analysis. In M. Darnell (Ed.), *Crytography and Coding* (1355 vol., pp. 30–45). Berlin Heidelberg: Springer. https://doi.org/10.1007/BFb0024447.

Bloustein, E. J. (1964). Privacy as an aspect of human dignity: An answer to Dean Prosser. *New York University Law Review, 39*, 962–1007. https://heinonline.org/HOL/P?h=hein.journals/nylr39&i=974

Bronitt, S., & Stellios, J. (2005). Telecommunications interception in Australia: Recent trends and regulatory prospects. *Telecommunications Policy*, *29*(11), 875–888. https://doi.org/10.1016/j.telpol.2005.06.010.

Butcher, M. P. (2009). At the foundations of information justice. *Ethics and Information Technology*, *11*(1), 57–69. https://doi.org/10.1007/s10676-009-9181-2.

Caproni, V. (2011). Statement Before the House Judiciary Committee, Subcommittee on Crime, Terrorism, and Homeland Security. https://archives.fbi.gov/archives/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies.

Carey, R. F., & Burkell, J. (2007). Revisiting the Four Horsemen of the Infopocalypse: Representations of anonymity and the Internet in Canadian newspapers. *First Monday*. https://doi.org/10.5210/fm.v12i8.1999

Carroll, P., & Windle, J. (2018). Cyber as an enabler of terrorism financing, now and in the future. *Journal of Policing Intelligence and Counter Terrorism*, *13*(3), 285–300. https://doi.org/10.1080/18335330.2018.1506149.

Chaum, D. (1985). Security without identification: Transaction systems to make big brother obsolete. *Communications of the ACM*, *28*(10), 1030–1044. https://doi.org/10.1145/4372.4373.

CISA (2014). *SSL 3.0 Protocol Vulnerability and POODLE Attack*. https://us-cert.cisa.gov/ncas/alerts/TA14-290A.

Cohen, S. (2002). *Folk devils and moral panics* (3rd ed.). Routledge.

Collins, J. P. (1997). Speaking in Code. *The Yale Law Journal*, *106*(8), 2691–2696. https://doi.org/10.2307/797231.

Comey, J. B. (2014). *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?* https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course

Communications Assistance for Law Enforcement Act 1994 (US).

Compliance with Court Orders Bill 2016 (US).

Comprehensive Counter-Terrorism Bill 1991 (US).

Cunningham, E. M. (2018). *Understanding rhetoric: A guide to critical reading and argumentation*. BrownWalker Press.

Curran, G., & Gibson, M. (2013). WikiLeaks, anarchism and technologies of dissent. *Antipode*, *45*(2), 294–314. https://doi.org/10.1111/j.1467-8330.2012.01009.x.

Daemen, J., & Rijmen, V. (2002). *The design of Rijndael, AES - the advanced encryption Standard*. Springer.

Daly, Y. M. (2014). The right to silence: Inferences and interference. *Australian & New Zealand Journal of Criminology*, *47*(1), 59–80. https://doi.org/10.1177/0004865813497732.

Dencik, L., Hintz, A., & Cable, J. (2016). Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data & Society*, *3*(2), 2053951716679678. https://doi.org/10.1177/2053951716679678.

Department of Justice (2021). FBI's encrypted phone platform infiltrated hundreds of criminal syndicates; result is massive worldwide takedown. https://www.justice.gov/usao-sdca/pr/fbi-s-encrypted-phone-platform-infiltrated-hundreds-criminal-syndicates-result-massive.

Diffie, W., & Hellman, M. E. (1977). Special Feature Exhaustive Cryptanalysis of the NBS Data Encryption. *Standard Computer, 10*(6), 74–84. https://doi.org/10.1109/C-M.1977.217750

Dolliver, D. S. (2015). Evaluating drug trafficking on the Tor network: Silk Road 2, the sequel. *International Journal of Drug Policy*, *26*(11), 1113–1123. https://doi.org/10.1016/j.drugpo.2015.01.008.

Dooley, J. F. (2018). *History of cryptography and cryptanalysis: Codes, ciphers and their algorithms*. Springer.

Dulay, N. B. M. (2019). The right to speak in code: A balancing of State Interest and the right to encrypted Speech. *University of Asia and the Pacific Law Journal*, *2*, 131–164.

Electronic Frontier Foundation (1998). About the Electronic frontier foundation's 'DES Cracker' Machine. https://web.archive.org/web/20170507231657/https://w2.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/HTML/19980716_eff_des_faq.html

Electronic Frontier Foundation (2021). *On Global Encryption Day, Let's Stand Up for Privacy and Security*. https://www.eff.org/deeplinks/2021/10/global-encryption-day-lets-stand-privacy-and-security

Ermoshina, K., Musiani, F., & Halpin, H. (2016). End-to-End Encrypted Messaging Protocols: An Overview. 9934 Vol. In F. Bagnoli, A. Satsiou, I. Stavrakakis, P. Nesi, G. Pacini, Y. Welp, T. Tiropanis, & D. DiFranzo (Eds.), *Internet Science* (pp. 244–254). Cham: Springer. https://doi.org/10.1007/978-3-319-45982-0_22

Express VPN. (2021). *The VPN that just works*. https://www.expressvpn.com/

Ferguson, N., Schneier, B., & Kohno, T. (2010). *Cryptography engineering: Design principles and practical applications*. Indianapolis, IN: Wiley.

Five Country Ministerial Communique (2018). Security coordination: Five country ministerial 2018. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/five-country-ministerial-2018

Formosa, P., Wilson, M., & Richards, D. (2021). A principlist framework for cybersecurity ethics. *Computers & Security*, *109*, 102382. https://doi.org/10.1016/j.cose.2021.102382.

Gray, D. (2019). A right to Go Dark. *SMU Law Review*, *72*(4), 621–668.

Guitton, C. (2013). A review of the available content on Tor hidden services: The case against further development. *Computers in Human Behavior*, *29*(6), 2805–2815. https://doi.org/10.1016/j.chb.2013.07.031.

Guru, A., & Ambhikar, A. (2020). A study of Cryptography to protect data from cyber-crimes. *Research Journal of Engineering and Technology*, *11*(2), 45–48. https://doi.org/10.5958/2321-581X.2020.00008.2.

Hartel, P., & van Wegberg, R. (2021). Going dark? Analysing the impact of end-to-end encryption on the outcome of Dutch criminal court cases. ArXiv:2104.06444 [Cs]. http://arxiv.org/abs/2104.06444.

Heeks, R., & Shekhar, S. (2019). Datafication, development and marginalised urban communities: An applied data justice framework. *Information Communication & Society*, *22*(7), 992–1011. https://doi.org/10.1080/1369118X.2019.1599039.

Hern, A. (2023). WhatsApp and Signal unite against online safety bill amid privacy concerns. *The Guardian*. https://www.theguardian.com/technology/2023/apr/18/whatsapp-signal-unite-against-online-safety-bill-privacy-messaging-apps-safety-security-uk.

Heron, S. (2009). Advanced Encryption Standard (AES). *Network Security, 2009*(12), 8–12. https://doi.org/10.1016/S1353-4858(10)70006-4

Hewson, E. C., & Harrison, P. S. (2021). Talking in the dark: Rules to facilitate open debate about lawful access to strongly encrypted information. *Computer Law & Security Review*, *40*, 105526. https://doi.org/10.1016/j.clsr.2020.105526.

Hochstrasser, D. (2021). *Encryption and the Privilege Against Self-Incrimination: What Happens When a Suspect Refuses to Divulge a Password* (SSRN Scholarly Paper ID 3921454). Social Science Research Network. https://papers.ssrn.com/abstract=3921454.

Holtfreter, R. E., & Harrington, A. (2015). Data breach trends in the United States. *Journal of Financial Crime*, *22*(2), 242–260. https://doi.org/10.1108/JFC-09-2013-0055.

Hutchings, A., & Holt, T. J. (2015). A crime script analysis of the online stolen data market. *British Journal of Criminology, 55*(3), 596–614. https://doi.org/10.1093/bjc/azu106. Table 1.

Investigatory Powers Act 2016 (UK).

Jalbert, K., Shields, D., Kelso, M., & Rubright, S. (2019). The power to plan: Mineral rights leasing, data justice, and proactive zoning in Allegheny County, Pennsylvania. *Environmental Sociology*, *5*(2), 164–176. https://doi.org/10.1080/23251042.2019.1624246.

Jardine, E. (2018). Tor, what is it good for? Political repression and the use of online anonymity granting technologies. *New Media & Society*, *20*(2), 435–452. https://doi.org/10.1177/1461444816639976.

Jardine, E. (2021). Policing the cybercrime script of darknet drug markets: Methods of effective law enforcement intervention. *American Journal of Criminal Justice*. https://doi.org/10.1007/s12103-021-09656-3.

Jarvis, C. (2020). *Crypto Wars: The fight for privacy in the Digital Age: A political history of digital encryption*. CRC Press.

Jarvis, C. (2021). Cypherpunk ideology: Objectives, profiles, and influences (1992–1998). *Internet Histories*. https://doi.org/10.1080/24701475.2021.1935547

Jayasinghe, D., Ragel, R., Ambrose, J. A., Ignjatovic, A., & Parameswaran, S. (2014). Advanced modes in AES: Are they safe from power analysis based side channel attacks? *2014 IEEE 32nd International Conference on Computer Design (ICCD)* (pp. 173–180). https://doi.org/10.1109/ICCD.2014.6974678.

Johnson, J. A. (2014). From open data to information justice. *Ethics and Information Technology*, *16*(4), 263–274. https://doi.org/10.1007/s10676-014-9351-8.

Jordan, T. (2015). *Information politics: Liberation and exploitation in the digital society*. Pluto Press.

Kahn, D. (1996). *The codebreakers: The comprehensive history of secret communication from ancient times to the internet* (2nd ed.). Scribner.

Kerr, O. S. (2019). Compelled decryption and the privilege against self-incrimination essays. *Texas Law Review*, *97*(4), 767–800.

Kerr, O. S., & Schneier, B. (2017). Encryption Workarounds. *Georgetown Law Journal*, *106*(4), 989–1020.

Kinna, R., & Prichard, A. (2019). Anarchism and non-domination. *Journal of Political Ideologies*, *24*(3), 221–240. https://doi.org/10.1080/13569317.2019.1633100.

Koops, B. J., & Kosta, E. (2018). Looking for some light through the lens of "cryptowar" history: Policy options for law enforcement authorities against "going dark. *Computer Law & Security Review*, *34*(4), 890–900. https://doi.org/10.1016/j.clsr.2018.06.003.

Kowalski, M., Hooker, C., & Barratt, M. J. (2019). Should we smoke it for you as well? An ethnographic analysis of a drug

cryptomarket environment. *International Journal of Drug Policy*, *73*, 245–254. https://doi.org/10.1016/j.drugpo.2019.03.011.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, *22*, 113–122. https://doi.org/10.1016/j.jisa.2014.09.005.

Kudla, C., & Paterson, K. G. (2005). Modular security proofs for key agreement protocols. In B. Roy (Ed.), *Advances in Cryptology—ASIACRYPT 2005* (3788 vol., pp. 549–565). Berlin Heidelberg: Springer. https://doi.org/10.1007/11593447_30.

Lauer, I., & Lauer, T. (2018). Undoing encryption: The argumentative function of metonyms. *Argumentation and Advocacy*, *54*(1–2), 53–71. https://doi.org/10.1080/00028533.2017.1420545.

Lawful Access to Encrypted Data Bill 2020 (US).

Lawson, N. (2009). Side-Channel attacks on Cryptographic Software. *IEEE Security Privacy*, *7*(6), 65–68. https://doi.org/10.1109/MSP.2009.165.

Levy, S. (2001). *Crypto: How the code rebels beat the government—Saving privacy in the digital age*. Penguin.

Li, B., Erdin, E., Gunes, M. H., Bebis, G., & Shipley, T. (2013). An overview of anonymity technology usage. *Computer Communications*, *36*(12), 1269–1283. https://doi.org/10.1016/j.comcom.2013.04.009.

Lyon, D. (2013). *The Information Society: Issues and illusions*. Wiley.

Macnish, K. (2018). *The ethics of surveillance: An introduction*. Routledge.

Mann, M. (2020). Technological Politics of Automated Welfare Surveillance: Social (and data) justice through critical qualitative Inquiry. *Global Perspectives*. https://doi.org/10.1525/gp.2020.12991

Mann, M., Daly, A., Wilson, M., & Suzor, N. (2018). The limits of (digital) constitutionalism: Exploring the privacy-security (im) balance in Australia. *International Communication Gazette*, *80*(4), 369–384. https://doi.org/10.1177/1748048518757141.

Maras, M. H. (2014). Inside darknet: The takedown of Silk Road. *Criminal Justice Matters*, *98*(1), 22–23. https://doi.org/10.1080/09627251.2014.984541.

Marthews, A., & Tucker, C. (2015). Government surveillance and internet search behavior. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564

Martin, J. (2014). Lost on the Silk Road: Online drug distribution and the cryptomarket. *Criminology & Criminal Justice*, *14*(3), 351–367. https://doi.org/10.1177/1748895813505234.

Martin, K. (2020). *Cryptography: The key to digital security, how it works, and why it matters*. W.W. Norton & Company.

Masco, J. (2010). Sensitive but Unclassified": Secrecy and the Counterterrorist State. *Public Culture*, *22*(3), 433–463. https://doi.org/10.1215/08992363-2010-004.

McAdow, J. E. (1966). Self-Incrimination: Testimonial vs. non-testimonial evidence. *Denver Law Journal, 43*(4), 501–510.

Menn, J. (2013). *Exclusive: Secret contract tied NSA and security industry pioneer.* https://www.reuters.com/article/us-usa-security-rsa-idUSBRE9BJ1C220131220

Meta (2023). *About*. https://www.whatsapp.com/about.

Miller, B. (2021). Is Technology Value-Neutral? *Science Technology & Human Values*, *46*(1), 53–80. https://doi.org/10.1177/0162243919900965.

Moore, D., & Rid, T. (2016). Cryptopolitik and the Darknet. *Survival*, *58*(1), 7–38. https://doi.org/10.1080/00396338.2016.1142085.

Newell, B. C. (2014). The massive metadata machine: Liberty, power, and secret mass surveillance in the U.S. and Europe. *Journal of Law and Policy for the Information Society, 10*(2), 481–522.

Nozick, R. (1974). *Anarchy, state, and utopia*. Basic Books.

O'Brien, M. (2014). The internet, child pornography and cloud computing: The dark side of the web? *Information & Communications Technology Law*, *23*(3), 238–255. https://doi.org/10.1080/13600834.2014.970376.

Office of Public Affairs (2020). *Virtual Five Country Ministerial Meeting—Joint Communiqué*. https://www.justice.gov/opa/pr/virtual-five-country-ministerial-meeting-joint-communiqu.

Ogasawara, M. (2022). Legalizing illegal mass surveillance: A transnational perspective on Canada's legislative response to the expansion of security intelligence. *Canadian Journal of Law and Society / Revue Canadienne Droit et Société*, *37*(2), 317–338. https://doi.org/10.1017/cls.2022.9.

Pednekar-Magal, V., & Shields, P. (2003). The State and Telecom Surveillance Policy: The Clipper Chip Initiative. *Communication Law and Policy*, *8*(4), 429–464. https://doi.org/10.1207/S15326926CLP0804_03.

Penney, J. W. (2015). Chilling effects: Online surveillance and Wikipedia use. *Berkeley Technology Law Journal*, *31*(1), 117–161. https://doi.org/10.15779/Z38SS13.

Petersen, J. (2015). Is code speech? Law and the expressivity of machine language. *New Media & Society*, *17*(3), 415–431. https://doi.org/10.1177/1461444813504276.

Pettit, P. (2011). The instability of freedom as non-interference: The case of Isaiah Berlin. *Ethics, 121*(4), 693–716.

Phelps, A., & Watt, A. (2014). I shop online – recreationally! Internet anonymity and Silk Road enabling drug use in Australia. *Digital Investigation*, *11*(4), 261–272. https://doi.org/10.1016/j.diin.2014.08.001.

Pitt, J. C. (2014). "Guns Don't Kill, People Kill"; Values in and/or Around Technologies. In P. Kroes & P.-P. Verbeek (Eds.), *The Moral Status of Technical Artefacts* (pp. 89–101). Springer. https://doi.org/10.1007/978-94-007-7914-3_6

Raz, J. (1986). *The morality of Freedom*. Clarendon.

Rodenstein, R. (2017). *Deputy Attorney General Rod J. Rosenstein Delivers Remarks on Encryption at the United States Naval Academy*. https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-encryption-united-states-naval

Rogaway, P. (2015). *The Moral Character of Cryptographic Work*. https://web.cs.ucdavis.edu/~rogaway/papers/moral-fn.pdf

Rozenshtein, A. Z. (2018). Wicked Crypto Women, Law, Society, & Technology Symposium. *UC Irvine Law Review, 9*(5), 1181–1216.

Ryan, J. M. (1996). Freedom to speak unintelligibly: The First Amendment Implications of Government-Controlled encryption. *William & Mary Bill of Rights Journal*, *4*(3), 1165–1222.

Sandywell, B. (2011). On the globalisation of crime: The internet and new criminality. In Y. Jewkes & M. Yar (Eds.), *Handbook of internet crime*. Willan Publishing.

Scheurer, K. (1995). The Clipper Chip: Cryptography Technology and the Constitution - the Government's answer to Encription chips away at constitutional rights note. *Rutgers Computer & Technology Law Journal*, *21*(1), 263–292.

Schneier, B. (2019). *Scaring people into supporting backdoors.* https://www.schneier.com/blog/archives/2019/12/scaring_people_.html

Šepec, M. (2020). *Revenge pornography or non-consensual dissemination of sexually explicit material as a sexual offence or as a privacy violation offence*. https://doi.org/10.5281/ZENODO.3707562.

Simone, M. A. (2009). Give me liberty and give me surveillance: A case study of the US government's discourse of surveillance. *Critical Discourse Studies*, *6*(1), 1–14. https://doi.org/10.1080/17405900802559977

Singh, S. (1999). *The code book: The science of secrecy from ancient Egypt to quantum crypgtography*. Anchor Books.

Soares, N. (2012). The right to remain encrypted: The self-incrimination doctrine in the Digital Age note. *American Criminal Law Review*, *49*(4), 2001–2020.

Sourbati, M., & Behrendt, F. (2021). Smart mobility, age and data justice. *New Media & Society*, *23*(6), 1398–1414. https://doi.org/10.1177/1461444820902682.

Spitters, M., Verbruggen, S., & Van Staalduinen, M. (2014). Towards a Comprehensive Insight into the Thematic Organization of the Tor Hidden Services. *2014 IEEE Joint Intelligence and Security Informatics Conference* (pp. 220–223). https://doi.org/10.1109/JISIC.2014.40.

Stallings, W. (2017). *Cryptography and network security: Principles and practices* (7th ed.). Pearson Education.

Standaert, F. X. (2010). *Introduction to Side-Channel Attacks*. https://perso.uclouvain.be/fstandae/PUBLIS/42.pdf.

Steinmetz, K. F., & Gerber, J. (2015). It doesn't have to be this way: Hacker perspectives on privacy. *Social Justice, 41*(3), 29–51.

Suzor, N., Pappalardo, K., & McIntosh, N. (2017). The passage of Australia's data retention regime: National security, human rights, and media scrutiny. *Internet Policy Review*. https://doi.org/10.14763/2017.1.454

Swire, P., & Ahmad, K. (2012). 'Going Dark' Versus a 'Golden Age for Surveillance.' *Centre for Democracy and Technology*. https://cdt.org/insights/%E2%80%98going-dark%E2%80%99-versus-a-%E2%80%98golden-age-for-surveillance%E2%80%99/

Taffel, S. (2015). We have never been Open: Activism and cryptography in Surveillance Societies. *MEDIANZ: Media Studies Journal of Aotearoa New Zealand*. https://doi.org/10.11157/medianz-vol14iss2id97

Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society, 4*(2), 2053951717736335. https://doi.org/10.1177/2053951717736335

Telecommunications Act 1997 (Austl)

Telecommunications (interception and security) Act 2013 (NZ).

Telegram (2021). *Telegram: A new era of messaging*. https://telegram.org/

Tor Project (2021). *About: History*. https://www.torproject.org/about/history/

Turner, S. (2014). Transport Layer Security. *IEEE Internet Computing*, *18*(6), 60–63. https://doi.org/10.1109/MIC.2014.126.

van der Bruggen, M., & Blokland, A. (2021). A crime script analysis of child sexual Exploitation Material Fora on the Darkweb. *Sexual Abuse*, *33*(8), 950–974. https://doi.org/10.1177/1079063220981063.

Vandenberg, D. T. (2017). Encryption served three ways: Disruptiveness as the key to exceptional access privacy/cyber security. *Berkeley Technology Law Journal, 32*(Annual Review Issue), 531–562.

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004.

Walden, I. (2018). The Sky is falling!' – responses to the 'Going dark' problem. *Computer Law & Security Review*, *34*(4), 901–907. https://doi.org/10.1016/j.clsr.2018.05.013.

Waldron, J. (1989). Rights in conflict. *Ethics*, *99*(3), 503–519.

Waldron, J. (2003). Security and Liberty: The image of balance. *Journal of Political Philosophy, 11*(2), 191–210. https://doi.org/10.1111/1467-9760.00174

Warren, S. D., & Brandeis, L. (1890). The right to privacy. *The Harvard Law Review, 4/5*, 193–220. Retrieved from https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

Weidman, M. (2017). Jurisdiction, the internet, and the good faith exception: Controversy over the Government's Use of Network Investigative Techniques comments. *Dickinson Law Review*, *122*(3), 967–996.

Weimann, G. (2016). Going Dark: Terrorism on the Dark web. *Studies in Conflict & Terrorism*, *39*(3), 195–206. https://doi.org/10.1080/1057610X.2015.1119546.

White House. (1994). *Statement of the Press Secretary*. Retrieved November 19, 2021 from https://archive.epic.org/crypto/clipper/white_house_statement_2_94.html.

Whitman, J. Q. (2004). The two Western cultures of privacy: Dignity versus liberty. *Yale Law Journal, 113*, 1151–1221.

Wray, C. (2017). *The FBI and the IACP: Bound Together by Partnership, Friendship, and Commitment*. https://www.fbi.gov/news/speeches/the-fbi-and-the-iacp-bound-together-by-partnership-friendship-and-commitment

Yoo, C. S. (2014). Toward a closer integration of law and computer science. *Communications of the ACM*, *57*(1), 33–35. https://doi.org/10.1145/2542503.

Zedner, L. (2007). Pre-crime and post-criminology? *Theoretical Criminology*, *11*(2), 261–281. https://doi.org/10.1177/1362480607075851.

Zimmerman, P. (1994). *PGP Source Code and Internals*. MIT Press.