McGill Law Journal
Revue de droit de McGill

Law Enforcement Access to Encrypted Data: Legislative Responses and the *Charter*

Steven Penney and Dylan Gibbs

Volume 63, Number 2, December 2017

URI: https://id.erudit.org/iderudit/1058192ar
DOI: https://doi.org/10.7202/1058192ar

See table of contents

Publisher(s)

McGill Law Journal / Revue de droit de McGill

ISSN

0024-9041 (print)
1920-6356 (digital)

Explore this journal

Cite this article

Penney, S. & Gibbs, D. (2017). Law Enforcement Access to Encrypted Data: Legislative Responses and the *Charter*. *McGill Law Journal / Revue de droit de McGill*, *63*(2), 201–245. https://doi.org/10.7202/1058192ar

Article abstract

In our digital age, encryption represents both a tremendous social benefit and a significant threat to public safety. While it provides the confidence and trust essential for digital communications and transactions, wrongdoers can also use it to shield incriminating evidence from law enforcement, potentially in perpetuity. There are two main legal reforms that have been proposed to address this conundrum: requiring encryption providers to give police "exceptional access" to decrypted data, and empowering police to compel individuals decrypt their own data.

This article evaluates each of these alternatives in the context of policy and constitutional law. We conclude that exceptional access, though very likely constitutional, creates too great a risk of data insecurity to justify its benefits to law enforcement and public safety. Compelled decryption, in contrast, would provide at least a partial solution without unduly compromising data security. And while it would inevitably attract constitutional scrutiny, it could be readily designed to comply with the *Charter*. By requiring warrants to compel users to decrypt and giving evidentiary immunity to the act of decryption, our proposal would prevent inquisitorial fishing expeditions yet allow the decrypted information itself to be used for investigative and prosecutorial purposes.

McGill Law Journal — Revue de droit de McGill

LAW ENFORCEMENT ACCESS TO ENCRYPTED DATA: LEGISLATIVE RESPONSES AND THE *CHARTER*

*Steven Penney and Dylan Gibbs**

In our digital age, encryption represents both a tremendous social benefit and a significant threat to public safety. While it provides the confidence and trust essential for digital communications and transactions, wrongdoers can also use it to shield incriminating evidence from law enforcement, potentially in perpetuity. There are two main legal reforms that have been proposed to address this conundrum: requiring encryption providers to give police "exceptional access" to decrypted data, and empowering police to compel individuals decrypt their own data.

This article evaluates each of these alternatives in the context of policy and constitutional law. We conclude that exceptional access, though very likely constitutional, creates too great a risk of data insecurity to justify its benefits to law enforcement and public safety. Compelled decryption, in contrast, would provide at least a partial solution without unduly compromising data security. And while it would inevitably attract constitutional scrutiny, it could be readily designed to comply with the *Charter*. By requiring warrants to compel users to decrypt and giving evidentiary immunity to the act of decryption, our proposal would prevent inquisitorial fishing expeditions yet allow the decrypted information itself to be used for investigative and prosecutorial purposes.

À l'ère du numérique, la cryptographie représente à la fois un avantage social considérable et une menace importante à la sécurité publique. Bien que cet outil assure la confiance essentielle à l'intégrité des communications et transactions numériques, des malfaiteurs peuvent également s'en servir pour dissimuler des preuves incriminantes des forces de l'ordre. Deux réformes juridiques ont été principalement proposées pour remédier à cette problématique: obliger les fournisseurs de systèmes cryptographiques à offrir à la police un « accès exceptionnel » aux données décryptées et à leur donner le pouvoir d'obliger les particuliers à décrypter leurs propres données.

Cet article évalue ces deux options dans le contexte de politiques publiques et du droit constitutionnel. Nous concluons que l'option de l'accès exceptionnel, bien que très probablement constitutionnelle, génère un risque d'insécurité trop important pour en justifier les avantages qu'il peut offrir aux forces de l'ordre et à la sécurité publique. Le déchiffrement forcé, en revanche, proposerait au moins une solution partielle à la problématique, sans compromettre indûment la sécurité des données visées. Et bien que cela attirerait inévitablement un examen constitutionnel, cela pourrait être facilement conçu pour se conformer à la *Charte*. En exigeant des mandats pour obliger les utilisateurs à décrypter leurs données et en donnant l'immunité en matière de preuve à l'acte de décryptage, notre proposition empêcherait les *expéditions de pêche inquisitoriales* tout en permettant l'utilisation des informations déchiffrées à des fins d'enquête et de poursuite.

* Steven Penney, Professor, Faculty of Law, University of Alberta. Dylan Gibbs, JD, University of Alberta, 2018; BSc (Computing Science), University of Alberta, 2013. Thanks to the three anonymous reviewers for their helpful comments.

Citation: (2017) 63:2 McGill LJ 201 — Référence : (2017) 63:2 RD McGill 201

Introduction

Encryption is one of the most important technologies of the digital age. It provides individuals and organizations with the confidence and trust necessary for a myriad of socially productive transactions, including e-commerce, personal and business communications, and the provision of government services.[1] It also facilitates the expression of ideas and opinion and pursuit of fulfilling lifestyle choices essential to a free and liberal society.[2]

But encryption also poses a tangible threat to public safety. Criminals and other wrongdoers use it to shield incriminating evidence from law enforcement. In response, police have had to find ways to circumvent it. Current methods are limited, however, and their success often depends on variables outside of law enforcement's control. To the extent that evidence of crime is increasingly in digital, encrypted form, it will often be either unavailable to police or require costly measures to access. This situation has no analogue in the pre-digital world: no safe or lock could permanently prevent police from lawfully obtaining incriminating documents or records stored within.[3] Encryption technology thus threatens to impede the detection and deterrence of crime and cause significant harm to society.[4]

Legislative responses to this conundrum may be grouped into three categories. The first is to do nothing, relying on existing and future investigative and technical methods to lawfully access as much encrypted data as possible. Whether this is a tenable situation for society involves many

---

1 See Sunny Handa, *Fundamentals of Information Technology* (Markham: LexisNexis Butterworths, 2004) at 135–37; Public Safety Canada, *Our Security, Our Rights: National Security Green Paper, 2016*, Background Document, Catalog No PS4-204/2016E-PDF (2016) at 60, online: <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016-bckgrndr/ntnl-scrt-grn-ppr-2016-bckgrndr-en.pdf> [*Green Paper*]; Industry Canada, *A Cryptography Policy Framework for Electronic Commerce: Building Canada's Information Economy and Society*, by the Task Force on Electronic Commerce (Ottawa: Industry Canada, 1998) at 1–2; Sang Ah Kim, "HTTPS: Staying Protected on the Internet" (2016) 1:1 Georgetown L Technology Rev 119 at 120.

2 See David Kaye, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UNGAOR, 29th Sess, UN Doc A/HRC/29/32 (2015) at para 12 [Kaye Report]. See also National Academies of Sciences, Engineering, and Medicine, *Decrypting the Encryption Debate: A Framework for Decision Makers* (Washington, DC: National Acadamies Press, 2018) ch 3.

3 See Dan Terzian, "Forced Decryption as Equilibrium: Why It's Constitutional and How *Riley* Matters" (2015) 109:4 Nw UL Rev 1131 at 1133, 1139.

4 See Orin S Kerr, "An Equilibrium-Adjustment Theory of the Fourth Amendment" (2011) 125:2 Harv L Rev 476 at 481–82 [Kerr, "Equilibrium"]. See also Orin S Kerr, "Searches and Seizures in a Digital World" (2005) 119:2 Harv L Rev 531.

difficult empirical and policy questions that we do not attempt to answer in this article.[5]

Should Parliament decide to act, two approaches present themselves. First, Parliament could choose to regulate the production and use of encryption technologies to enhance law enforcement's lawful access to unencrypted information. Such an "exceptional access" regime would compel encryption providers to give police "backdoor" access to decrypted data. The second approach would empower police to compel individuals—by imposing sanctions for refusal—to decrypt their own data. This could be achieved by compelling users to give police passwords, encryption keys, biometric identifiers, or the unencrypted data itself.[6]

Both of these legislative solutions raise concerns. Exceptional access presents technical challenges, including the risk that malicious actors will exploit security vulnerabilities intended only for legitimate law-enforcement purposes.[7] Compelled decryption avoids this risk, but raises concerns relating to privacy and self-incrimination.[8]

This article evaluates each of these alternatives in the context of policy and constitutional law. We conclude that exceptional access, though very likely constitutional, creates too great a risk of data insecurity to justify its benefits to law enforcement and public safety. Compelled decryp-

---

5 For differing views on this debate, see James B Comey, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?" (16 October 2014), online: <https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course>, archived at https://perma.cc/WEE8-JGWC; Matthew G Olsen et al, "Don't Panic: Making Progress on the 'Going Dark' Debate" (2016) Berkman Center for Internet & Society, online: <cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf>. See also National Academies of Sciences, Engineering, and Medicine, *supra* note 2.

6 See generally *Green Paper*, *supra* note 1 at 60–61.

7 See e.g. Harold Abelson et al, "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications" (2015) MIT Computer Science and Artificial Intelligence Laboratory Technical Report MIT-CSAIL-TR-2015-026 at 15, online: <hdl.handle.net/1721.1/97690>, archived at https://perma.cc/9BXA-AEMB; Tim Cook, "A Message to Our Customers" (16 February 2016), online: <https://www.apple.com/customer-letter>, archived at https://perma.cc/9VSH-XZFG; Kaye Report, *supra* note 2 at para 42.

8 See *Green Paper*, *supra* note 1 at 61; Office of the Privacy Commissioner of Canada, "Consultation on Canada's National Security Framework: Submission of the Office of the Privacy Commissioner of Canada to the National Security Policy Directorate of Public Safety Canada" (5 December 2016), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_psc_161205>, archived at https://perma.cc/7636-GB55 [Office of the Privacy Commissioner of Canada, "Consultation"]. See also *R c Boudreau-Fontaine*, 2010 QCCA 1108 at para 39, [2010] QJ No 5399 (QL) [*Boudreau-Fontaine*].

tion, in contrast, would provide at least a partial solution to the encryption problem without unduly compromising data security. And while it would inevitably attract constitutional scrutiny, it could be readily designed to cohere with the *Canadian Charter of Rights and Freedoms*.[9] By requiring warrants to compel users to decrypt their data, and by giving evidentiary immunity to the act of decryption, our proposal would prevent inquisitorial fishing expeditions yet allow the decrypted information to be used for investigative and prosecutorial purposes.

The article proceeds as follows. Part I outlines existing methods for circumventing encryption and their limitations. Part II discusses the legal and policy issues surrounding the exceptional access and compelled disclosure alternatives. We argue that the latter is the more viable policy option, can be designed to comply with the *Charter*'s self-incrimination and privacy protections, and would maintain the contemporary balance between liberty and crime control interests.[10]

I. Existing Methods of Defeating Encryption

Encryption uses the process of cryptography to transform ordinary information, or plaintext, into unintelligible ciphertext. Persons who possesses the encrypted ciphertext cannot recover the plaintext information unless they know both the algorithm used to perform the transformation and an additional piece of information called the encryption key.[11] In effect, this allows encryption to hide information from anyone not authorized to view it.

The theoretical security of an encryption system is determined by considering whether it can be broken using a reasonable amount of time and computing power. While any encryption can be defeated by trying every possible key, any algorithm that requires an unreasonable amount of time and resources to break is considered computationally secure.[12]

---

9 Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11 [*Charter*].

10 See generally Kerr, "Equilibrium", *supra* note 4 (arguing that constitutional rights should be interpreted to preserve the balance of interests prevailing before the adoption of technologies that threaten to upset that balance).

11 See Niels Ferguson, Bruce Schneier & Tadayoshi Kohno, *Cryptography Engineering: Design Principles and Practical Applications* (Indianapolis: Wiley, 2010) at 23–24.

12 See Jon Erickson, *Hacking: The Art of Exploitation*, 2nd ed (San Francisco: No Starch Press, 2008) at 396. The Advanced Encryption Standard (AES), for example, is a common encryption implementation that can support a 256-bit key. The total number of possible 256-bit combinations is one followed by seventy-seven zeros. On the current

Even computationally secure encryption, however, may be vulnerable to attack. The encryption algorithm and keys are part of a larger security system that may contain weaknesses.[13] Depending on the algorithm used, the device it operates on, and decisions made by the user, police may be able to recover the plaintext information without acquiring the encryption key. Moreover, many systems derive the key from a user-selected password.[14] In such instances, the encryption is only as strong as the user's choice of password.

As mentioned, police do currently have methods of accessing encrypted data. These may be grouped into four categories: (i) traditional investigative methods; (ii) third party assistance; (iii) exploiting vulnerabilities; and (iv) guessing the password.[15] As detailed below, however, each has significant limitations. Without exceptional access or compelled disclosure, law-enforcement will continue to be prevented from accessing information that they are legally entitled to obtain.

A. Traditional Investigative Methods

Police may use several traditional investigative techniques to obtain plaintext from encrypted data, most commonly through surveillance, search and seizure, and questioning.[16] As its name implies, surveillance involves surreptitiously observing suspects to capture passwords, encryption keys, or plaintext before it is encrypted. Hidden video cameras, for

---

state of technology, an attacker would not be able to guess that length of a key in a lifetime, making AES-256 computationally secure.

13 See Ferguson, Schneier & Kohno, *supra* note 11 at 4–7, 24–25; Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World* (Indianapolis: Wiley, 2015) at 84 [Schneier, *Secrets*].

14 *Ibid* at 105.

15 For a slightly different categorization encompassing the same techniques, see Orin S Kerr & Bruce Schneier, "Encryption Workarounds" (2018) 106:4 Geo LJ 989 at 996ff.

16 Encrypted ciphertext provides very little investigative or prosecutorial value unless law enforcement can defeat the encryption and recover the corresponding plaintext. As there are many legitimate uses of encryption, the fact that information is encrypted cannot, without more, be used to infer that an accused is guilty of an offence. See e.g. *R v Sonne*, 2012 ONSC 2126, [2012] OJ No 2160 (QL) ("even if I were to conclude that Mr. Sonne had encrypted a portion of his hard drive, that does not mean that he did so for nefarious purposes. ... I, therefore, am not prepared to draw any adverse inference from the fact that Mr. Sonne may have encrypted a portion of his hard drive" at paras 18–19). In limited circumstances, however, encrypted information can have some evidentiary value even in the absence of the corresponding plaintext. See e.g. *R v CMM*, 2012 MBQB 141, 93 CR (6th) 155 (where there was testimony that the accused took five pornographic images of a child and evidence that five images removed from camera, the court inferred that the encrypted drive recovered from accused's residence contained the images even though police could not break encryption).

example, may record suspects' encryption keys or passwords as they are inputted into the device. In addition, if suspects share passwords over unencrypted channels, police can potentially intercept them in transit. And most effectively, police can obtain keys or plaintext by surreptitiously installing software on suspects' devices. The most common form is a "keylogger", which records all keystrokes, including passwords, entered on a device.[17] Similarly, any plaintext information input through keystrokes would be recorded before it is encrypted. Another type of software, known as a "rootkit", can provide full access to a targeted device, making plaintext information directly recoverable.[18]

Surveillance methods have at least three major limitations. First, they require police to have pre-existing knowledge that a suspect is using a particular device. Surveillance thus is inapplicable when police discover a device previously unknown to them. Second, even when a device is targeted in advance, it will often be difficult to surreptitiously capture inputted data. Observing a password, whether in person or through video surveillance, presents logistical challenges for police.[19] Similarly, software tools need to be secretly installed on a suspect's device. Doing this by gaining physical access to the device involves the same challenges discussed above. And remote installation requires exploiting security vulnerabilities that, as discussed in greater detail below, may either be prohibitively costly to overcome or may not even exist.[20] Finally, surveillance is often highly intrusive, potentially recording information, communications, and activities far beyond what is necessary to defeat encryption, including that relating to innocent third parties.[21] Police wishing to conduct such surveil-

---

17 See Sara M Smyth, *Cybercrime in Canadian Criminal Law*, 2nd ed (Toronto: Carswell, 2015) at 188. For an example of police using a keylogger, see *United States v Scarfo*, 180 F Supp (2d) 572 at 574–76 (D NJ 2001).

18 See Reverend Bill Blunden, *The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System*, 2nd ed (Burlington, Mass: Jones & Bartlett Learning, 2013) at 4–5.

19 Mobile devices are especially difficult to observe through physical surveillance, as there is no fixed location to observe, and devices protected by biometric security are wholly immune to such efforts.

20 The use and availability of exploits is discussed below in Part I.C. See generally Steven M Bellovin et al, "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet" (2014) 12:1 Northwestern J Technology & Intellectual Property 1 (discussing law enforcement's use of weaknesses to gain access to online systems); Orin Kerr, "Government 'Hacking' and the Playpen Search Warrant", *The Washington Post* (27 September 2016), online: <https://www.washingtonpost.com>, archived at https://perma.cc/8UHG-TAWL (network investigative technique "was used to bypass the anonymizing feature of Tor ... and retrieve the real IP address that Tor had hidden").

21 See generally *R v Thompson*, [1990] 2 SCR 1111, 73 DLR (4th) 596 [*Thompson* cited to SCR] (noting the intrusiveness of wiretap authorizations for public pay phones, which may intercept communications of large numbers of non-targets).

lance must meet onerous standards of justification under the *Criminal Code*[22] and *Charter*.[23]

Alternatively, police may use search and seizure powers to locate either the user's password or a copy of the targeted plaintext information. Some people record their passwords to avoid having to memorize them.[24] If police are authorized to search locations where users store their passwords and find them, they can use them to access the encrypted information it protects.[25] In addition, copies of the targeted data may be stored in another location that is either unencrypted or accessible by third parties.[26] Lastly, po-

---

22 RSC 1985, c C-46 [*Criminal Code*]. Depending on the circumstances, the use of surveillance software would require either a warrant under s 487.01 or an authorization under Part VI of the *Criminal Code* (ss 183–86). Briefly, the former authorizes searches and seizures not otherwise provided under the *Code* if there are "reasonable grounds to believe" that an offence has been committed and that evidence concerning the offence will be obtained through the use of surveillance. The surveillance must also be in the "best interests of the administration of justice." See generally *R v Araujo*, 2000 SCC 65, [2000] 2 SCR 992 [*Araujo*]. The latter regulates the interception of "private communications". In addition to the requirements for s 487.01 warrants, intercept authorizations are available only for certain listed offences and must (generally) meet the standard of "investigative necessity."

23 See generally *R v Duarte*, [1990] 1 SCR 30, 65 DLR (4th) 240 [*Duarte* cited to SCR]; *Thompson*, *supra* note 21.

24 See e.g. *R v Nero*, 2016 ONCA 160 at paras 134, 153, 345 OAC 282 [*Nero*]. The location of a recorded password could be physical, such as a sticky note, or digital, such as a password file on a computer. Some internet browsers and other software applications, for example, permit users to store all of their passwords in a central location. See e.g. "Manage Saved Passwords", *Google Chrome Help*, online: <https://support.google.com/chrome/answer/95606>, archived at https://perma.cc/2A4E-7472.

25 See *Nero*, *supra* note 24.

26 The third party could be an individual (e.g. the recipient of an email or text message from a target) or a service provider. Methods for obtaining unencrypted data from third party service providers are discussed in Part I.B, below. In situations where device data, such as that on a mobile phone, is periodically backed on third party servers, such as Apple iCloud, police will typically be able to obtain plaintext from the third party. But police may still need access to the device if relevant evidence has not yet been uploaded. For example, in a widely publicized case dealing with the 2015 San Bernardino terrorist attack, the FBI recovered an iPhone and recovered a copy of its data that had been backed up to Apple's iCloud storage. This backup copy did not provide a full picture of the device's information, however, as it was not current to the date of the attack. Consequently, the FBI still sought to obtain the most recent device data. See Kerr & Schneier, *supra* note 15 at 1010–11; Michael Hack, "The Implications of Apple's Battle with the FBI" [2016] 7 Network Security 8 at 8; Russell Brandom, "Why Apple and the FBI Are Fighting over an iCloud Account", *The Verge* (22 February 2016), online: <https://www.theverge.com>, archived at https://perma.cc/KVE3-XMDU.

lice may be able to lawfully seize devices while they are in an "unlocked" state and retrieve the data they contain.[27]

These techniques are likely to be effective, however, only for naïve targets. More sophisticated wrongdoers can readily secure their passwords and data to thwart these techniques. Moreover, as mentioned, device manufacturers, software designers, and service providers are making it increasingly simple for ordinary users to adopt security best practices, often in the form of "default" settings that provide strong security without any action by the user.

Lastly, police may ask suspects to voluntarily provide passwords, encryption keys, biometric identifiers, or plaintext. So long as their questioning is lawful,[28] they may use any information revealed to access encrypted information in their possession.[29] But while police are trained to induce cooperation and may employ a considerable degree of pressure and manipulation,[30] there is no guarantee this method will succeed, especially in interrogating sophisticated wrongdoers. Suspects enjoy a freedom to remain silent in response to police questioning[31] and police cannot (currently) require them to assist with decryption.[32]

---

27 Warrants permitting unannounced entry may increase the likelihood of recovering data while a computer is powered on and unlocked. Unannounced entry is presumptively unreasonable, but the threat of encryption may justify an exception. See *R v Burke*, 2013 ONCA 424 at paras 41, 47, 50–51, 307 OAC 171.

28 The most significant restrictions on police questioning arise from the common law confessions rule, which applies to statements made to "persons in authority", and s 10(b) of the *Charter*, *supra* note 9, which gives suspects the right to speak to counsel on detention. See generally Steven Penney, Vincenzo Rondinelli & James Stribopoulos, *Criminal Procedure in Canada*, 2nd ed (Toronto: LexisNexis, 2018) ch 4.

29 When police obtain a password involuntarily under the confessions rule or through a violation of *Charter* rights, any evidence obtained may be excluded at trial. See e.g. *R v Stemberger*, 2012 ONCJ 31 at paras 125–29, 254 CRR (2d) 1.

30 See generally *R v Spencer*, 2007 SCC 11, [2007] 1 SCR 500; *R v Oickle*, 2000 SCC 38, [2000] 2 SCR 3 [*Oickle*].

31 See *R v Singh*, 2007 SCC 48 at para 27, [2007] 3 SCR 405 [*Singh*]; *R v Turcotte*, 2005 SCC 50 at para 41, [2005] 2 SCR 519; Ed Ratushny, *Self-incrimination in the Canadian Criminal Process* (Toronto: Carswell, 1979) at 185–86.

32 Some have suggested that assistance orders under s 487.02 of the *Criminal Code*, *supra* note 22 could be used to compel suspects to disclose encryption keys. See Office of the Privacy Commissioner of Canada, News Release, "Don't Repeat Past Mistakes, Privacy Commissioner Warns as Government Reviews National Security Framework", (6 December 2016), online: <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2016/nr-c_161206>, archived at https://perma.cc/X285-GMUH. That provision empowers a judge or justice to "order a person to provide assistance, if the person's assistance may reasonably be considered to be required to give effect to [an] authorization or warrant." In our view, however, courts are unlikely to interpret this provision to compel suspects to assist with decrypting their own data, especially as such compulsion impli-

B. Third Party Assistance

If police cannot access encrypted information themselves or convince suspects to help decrypt it, a logical place for them to turn to is the organization that implemented the encryption. The extent to which third parties can assist with decryption differs depending on the form of encryption used. End-to-end encryption is initiated on the user's device, and protects data from any third party coming into possession of it, including telecommunications, internet, and software application providers.[33] It presents police with a more challenging obstacle than encryption initiated by such technology service providers. When providers encrypt information, they control the keys and can access the plaintext at any time.[34] But they cannot access information encrypted end-to-end without additional weak-

---

cates self-incrimination and privacy concerns under the *Charter*. See *Boudreau-Fontaine*, *supra* note 8 at paras 45–46. But see *R v Talbot*, 2017 ONCJ 814, 2017 CarswellOnt 19113 (WL Can), leave to appeal to SCC refused, 37902 (5 April 2018) (suggesting that suspects may be subject to assistance orders but holding that an order compelling a physical "gesture" passcode violated s 7 of the *Charter*). In contrast, as discussed in Part I.B, below, s 487.02 may potentially be used to require third party service providers to decrypt data if they are able to so.

While police have no power to compel decryption, customs agents likely do. Several provisions in the *Customs Act* require persons entering Canada and importers of goods to truthfully answer agents' questions. See e.g. *Customs Act*, RSC 1985, c 1 (2nd Supp), ss 11, 11.4, 13, 22, 40. Courts have held that these provisions do not violate the *Charter* when deployed as part of "routine questioning" at the border. See *R v Jones* (2006), 81 OR (3d) 481 at 491–93, 211 CCC (3d) 4 (CA). Courts have also held that customs agents may use these powers to compel device passwords without violating s 7 of the *Charter*. See *R v Buss*, 2014 BCPC 16 at para 33, 301 CRR (2d) 309. See also *R v Whittaker*, 2010 NBPC 32, 367 NBR (2d) 334 (upholding a customs officer's demand for a password without mentioning s 7 of Charter). See generally Steven Penney, "'Mere Evidence'? Why Customs Searches of Digital Devices Violate Section 8 of the *Charter*" (2016) 49:2 UBC L Rev 485 at 503–04; Robert J Currie, "Electronic Devices at the Border: The Next Frontier of Canadian Search and Seizure Law?" (2016) 14:2 CJLT 289 at 313–16.

33 See Mohamed Nabeel, "The Many Faces of End-to-End Encryption and Their Security Analysis" in Andrzej M Goscinski & Min Luo, eds, *2017 IEEE 1st International Conference on Edge Computing* (Los Alamitos, California: Institute of Electrical and Electronics Engineers, 2017) 252 at 252; Joris VJ van Hoboken & Ira S Rubinstein, "Privacy and Security in the Cloud: Some Realism about Technical Solutions to Transnational Surveillance in the Post-Snowden Era" (2014) 66:2 Me L Rev 487 at 516; Andy Greenberg, "Hacker Lexicon: What Is End-to-End Encryption?", *Wired* (25 November 2014), online: <https://www.wired.com>, archived at https://perma.cc/R6CQ-G8HQ.

34 Apple, for example, encrypts information stored through its iCloud service. Faced with a lawful demand, Apple can decrypt and produce this information. See Apple, "Legal Process Guidelines: Government & Law Enforcement Outside the United States" ("[a]ll iCloud content data stored by Apple is encrypted at the location of the server. ... Apple retains the encryption keys in its US data centres" at 9) online: <https://images.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf>.

nesses built into the system.[35] Unless providers store a copy of the encryption key or retain some way of determining it, police will not be able to access the user's information.

The same principles apply to encrypted data stored on a user's device. Secure device encryption systems, such as those used on the latest mobile operating systems developed by Google and Apple, ensure that the service providers do not have access to the user's encryption key.[36] For both end-to-end and secure device encryption, the implications are the same. Without building vulnerabilities into the system, service providers are in no better position to access encrypted information than the police.

Police currently have two ways to obtain third party assistance with decryption, neither of which works for end-to-end or secure device encryption. First, as detailed in Part II.A below, wireless telecommunications providers are required to provide plaintext versions of data they have encrypted when police demonstrate their lawful entitlement to that data. But providers are not obliged—and in any case, would not likely have the capacity—to provide plaintext of data encrypted before entering the network, as with data encrypted end-to-end by a user or by default on a device.

Second, police may ask any service provider, such as a device manufacturer, to voluntarily assist with the decryption of data that they have encrypted (or facilitated the encryption of). If they do not comply voluntarily, police might be able to use section 487.02 of the *Criminal Code* to force them to do so. That provision authorizes a judge or justice to "order a person to provide assistance, if the person's assistance may reasonably be considered to be required to give effect to [an] authorization or warrant." Though there are no reported decisions applying this provision in this context, there are reports that police have used it in attempts to obtain decrypted data from service providers.[37]

---

[35] One such end-to-end communication encryption system available to consumers is the popular messaging application WhatsApp. See WhatsApp, "WhatsApp Security", online: <https://www.whatsapp.com/security>, archived at https://perma.cc/4968-FR4R.

[36] See Apple, "iOS Security: iOS 11", (January 2018) at 12, online: <https://www.apple.com/business/docs/iOS_Security_Guide.pdf> [Apple, "iOS Security"]; Google, "Android 7.1 Compatibility Definition" (21 June 2017) at 79, online: <https://source.android.com/compatibility/7.1/android-7.1-cdd.pdf>. See also Orin Kerr, "Apple's Dangerous Game", *The Washington Post* (19 September 2014) online: <https://www.washingtonpost.com>, archived at https://perma.cc/M84G-BWWN [Kerr, "Dangerous Game"].

[37] For example, in *R v Mirarchi* the RCMP sought Research in Motion's help to read encrypted communications. The redacted court documents indicate that the RCMP obtained the global Blackberry encryption key, but do not reveal whether Research in Mo-

As end-to-end and secure device encryption become more common, however, the usefulness of assistance orders is likely to wane.[38] Further, many providers have taken the position that these orders cannot be used to compel them to attempt to defeat their own encryption systems.[39] It is

---

tion provided the key in response to the existing assistance order. See *R v Mirarchi* (18 November 2015), Laval, 540-01-063428-141 (motion for disclosure of information) (Qc Sup Ct) online: <https://cippic.ca/uploads/R_v_Mirarchi-QCCS-18Nov2015.pdf>; Justin Ling & Jordan Pearson, "Exclusive: Canadian Police Obtained BlackBerry's Global Decryption Key", *Vice News* (14 April 2016), online: <https://news.vice.com>, archived at https://perma.cc/D4VF-MQMU. See also Office of the Privacy Commissioner of Canada, "Consultation", *supra* note 8 ("[i]t should be noted that Canada is not without rules which may assist law enforcement agencies in addressing encryption issues. ... [Assistance order provisions] have been used in investigations to defeat security features or compel decryption keys"); Clayton Rice, "Apple and 'Assistance Orders' in Canada" (8 November 2015), *On The Wire* (blog), online: <https://www.claytonrice.com/apple-and-assistance-orders-in-canada>, archived at https://perma.cc/KX2R-PNRL; United States, Library of Congress, "Government Access to Encrypted Communications: Canada", by Tariq Ahmad (May 2016), online: <www.loc.gov/law/help/encrypted-communications/canada.php>, archived at https://perma.cc/F8ZD-VYEU.

Some have also suggested that police may compel providers to assist with decryption under s 487.012 of the *Criminal Code*, *supra* note 22. See Christopher Parsons & Tamir Israel, "Canada's Quiet History of Weakening Communications Encryption" (11 August 2015), online: Telecom Transparency Project <www.telecomtransparency.org/canadas-quiet-history-of-weakening-communications-encryption>, archived at https://perma.cc/NY2H-5G43. That provision allows police to demand the preservation of computer data without a warrant when they have a reasonable suspicion that the data will assist an investigation. S 487.012(5) permits police to "impose any conditions in the demand that they consider appropriate—including conditions prohibiting the disclosure of its existence or some or all of its contents." Parsons and Israel read the latter provision as enabling the preservation and disclosure of decryption keys, and as potentially empowering police to "develop new decryption capacities." This interpretation is not plausible. Neither s 487.012 nor the provision authorizing police to ultimately obtain the data under judicial authorization—a production order under s 487.014 of the *Criminal Code*, *supra* note 22—refer to encryption in any way. Further, the authors' reading would grossly exceed s 487.012's clear purpose, which is merely to prevent the loss of evidence before it can be acquired by court order. #

38 See Danny Yadron, "Facebook, Google and WhatsApp Plan to Increase Encryption of User Data", *The Guardian* (14 March 2016), online: <https://www.theguardian.com>, archived at https://perma.cc/F8XR-KL73; Lily Hay Newman, "Skype's Rolling Out End-to-end Encryption for Hundreds of Millions of People", *Wired* (1 January 2018), online: <https://www.wired.com>, archived at https://perma.cc/LJ4D-PYW6.

39 See e.g. Cook, *supra* note 7; Apple, Press Release, "Amicus Briefs in Support of Apple" (2 March 2016), online: Apple <https://www.apple.com/newsroom/2016/03/03Amicus-Briefs-in-Support-of-Apple>, archived at https://perma.cc/UFQ3-WSMJ; Chris Welch, "Google's CEO Just Sided with Apple in the Encryption Debate", *The Verge* (17 February 2016), online: <https://www.theverge.com>, archived at https://perma.cc/SAT3-NKJD; Amul Kalia, "Where Do Major Tech Companies Stand on Encryption?", (9 October 2015), online: Electronic Frontier Foundation <https://www.eff.org/deeplinks/2015/10/where-do-major-tech-companies-stand-encryption>, archived at https://perma.cc/8KXR-MHKY.

likely, therefore, that police will be increasingly unable to enlist service providers to decrypt data.[40]

C. Exploiting Vulnerabilities

Another way for law enforcement agencies to access encrypted information is through technical vulnerabilities, or exploits, within an encryption system. These weaknesses can exist in the encryption algorithm, on the device that the algorithm operates on, or within other applications on the same device. To discover such exploits, state agencies can either develop their own hacking capabilities or purchase them from third party vendors.[41] For example, the FBI used a purchased exploit to access data on an Apple device used by a perpetrator of the 2015 San Bernardino terrorist attack. The exploit disabled security measures built into the device that prevented the agency from using "brute-force" computation to guess its password.[42] Some encryption implementations also store keys on the device, leaving them vulnerable to recovery by resourceful attackers.[43]

Police may only exploit vulnerabilities, however, before the encryption provider fixes them. Technology companies have strong commercial reasons to maximize data security. They therefore invest heavily in preventing and quickly redressing vulnerabilities.[44] While efforts to reduce vul-

---

40 See Kerr & Schneier, *supra* note 15 at 1018.

41 Zerodium is one example of an exploit vendor; it will currently pay up to US$1.5M for software exploits that are unknown to the software vendor. Zerodium then resells these exploits to "mainly government organizations in need of specific and tailored cybersecurity capabilities, as well as major corporations from defense, technology, and finance sectors, in need of protective solutions to defend against zero-day attacks." See Zerodium, "Questions and Answers", online: <https://zerodium.com/faq.html>, archived at https://perma.cc/GBQ8-G8YD; Zerodium, "Our Exploit Acquisition Program", online: <https://zerodium.com/program.html>, archived at https://perma.cc/8WUH-6ZNA.

42 See Haje Jan Kamps, "San Bernardino iPhone was Hacked Using a Zero-day Exploit", *TechCrunch* (12 April 2016), online: <https://techcrunch.com>, archived at https://perma.cc/D5E6-P962. A similar exploit is known to exist within certain versions of the Android operating system. See Mohit Kumar, "How to Crack Android Full Disk Encryption on Qualcomm Devices", *The Hacker News* (1 July 2016), online: <https://thehackernews.com>, archived at https://perma.cc/9MAJ-8W4Z. The technique of guessing a device password through brute force is discussed under Part I.D, below.

43 See J Alex Halderman et al, "Lest We Remember: Cold-Boot Attacks on Encryption Keys", (2009) 52:5 Communications of the ACM 91, DOI: <10.1145/1506409.1506429>; Sebastian Anthony, "How to Bypass an Android Smartphone's Encryption and Security: Put It in the Freezer", *Extreme Tech* (12 March 2013), online: <https://www.extremetech.com>, archived at https://perma.cc/AQ36-8SJJ.

44 For example, several technology companies have established "bug bounty" programs that pay researchers who uncover vulnerabilities. See Mingyi Zhao, Aron Laszka & Jens Grossklags, "Devising Effective Policies for Bug-Bounty Platforms and Security Vulnerability Discovery" [2017] 7 J Information Policy 372; Andreas Kuehn & Milton

nerabilities are not always successful,[45] developing a toolkit of unaddressed exploits demands significant resources and technical expertise.[46]

Exploiting vulnerabilities also raises a broader policy concern. Government-developed hacking tools can be leaked or stolen and subsequently used by malicious actors.[47] And police purchases of third party exploits spur the market for privately developed hacking tools, which again may also be used for nefarious purposes. In other words, state-sponsored hacking, even if targeted only at likely wrongdoers, may effectively diminish the security of encryption for law-abiding citizens.[48]

D. Guessing the Password

Lastly, police may attempt to guess the user's encryption key or password. Current encryption standards are so strong that it is rarely possible to discover the key within reasonable time and resource limits.[49] But be-

---

Mueller, "Analyzing Bug Bounty Programs: An Institutional Perspective on the Economics of Software Vulnerabilities" (Working Paper delivered at the 2014 TPRC/42nd Research Conference on Communication, Information and Internet Policy, George Mason University School of Law, Arlington, Virginia, September 12–14 2014 [unpublished]) at 3–4, online: SSRN <ssrn.com/abstract=2418812>; Andrea Peterson, "Inside the Economics of Hacking", *The Washington Post* (5 November 2015), online: <https://www.washingtonpost.com>, archived at https://perma.cc/7HGU-GUR8.

45 Software vendors uncover and patch many vulnerabilities, but those patches often still contain errors and do not address all existing security holes. Moreover, patches produced by software vendors are useful only when they are installed by the end user. See Jay P Kesan & Carol M Hayes, "Bugs in the Market: Creating a Legitimate, Transparent, and Vendor-Focused Market for Software Vulnerabilities" (2016) 58:3 Ariz L Rev 753 at 787.

46 See Kerr & Schneier, *supra* note 15 at 1006. For example, the FBI reportedly paid US$900,000 for a third party exploit to gain access to an encrypted phone. See Matt Novak, "The FBI Paid $900,000 to Unlock the San Bernardino Terrorist's iPhone", *Gizmodo* (8 May 2017), online: <https://gizmodo.com>, archived at https://perma.cc/7RW5-8BNU.

47 A group called the Shadow Brokers, for example, obtained several hacking tools from the US National Security Agency (NSA) and released them publicly. These exploits were subsequently used in a large-scale cyberattack on Ukranian organizations, as well as in a worldwide ransomware attack. See Nicole Perlroth & David E Sanger, "Hackers Hit Dozens of Countries Exploiting Stolen NSA Tool", *The New York Times* (12 May 2017), online: <https://www.nytimes.com>, archived at https://perma.cc/9HWA-ZLGL; Lily Hay Newman "Latest Ransomware Hackers Didn't Make WannaCry's Mistakes", *Wired* (27 June 2017), online: <https://www.wired.com>, archived at https://perma.cc/Y6DA-QB62.

48 See Bellovin et al, *supra* note 20 at 47–48.

49 See Kerr & Schneier, *supra* note 15 ("[i]n the arms race between encryption and brute-force attacks, the mathematics overwhelmingly favors encryption" at 994).

cause many encryption systems derive their key from a user-selected password, police can often devote their energies to the easier task of guessing it.[50]

There are two main ways to guess a password: trying all possible combinations (a brute-force attack) and trying a list of passwords (a dictionary attack).[51] The probability of success for each method turns on the strength of the encryption system and complexity of the password, as well as the computational resources available to police.

Success is more likely when the number of potential passwords is limited. For example, a four-digit numeric pin allows for only 10,000 combinations, while a four-character alphanumeric password—using only numbers and lowercase letters—allows for 1,679,616. However, even when the number of combinations is small, the system may include countermeasures designed to thwart repeated password entry attempts. If the relevant encrypted files can be extracted from the device and run on powerful offline processors, a great many passwords can be tried within a short period of time.[52] But some systems implement controls to prevent such external password cracking attempts, forcing the attacker to make all attempts directly on the targeted device. Depending on the device, this can drastically increase the amount of time required to complete a brute-force attack.[53] On other systems, users can employ a setting whereby data is permanently destroyed if an incorrect password is entered a certain num-

---

50 *Ibid* at 997–1000.

51 See Schneier, *Secrets*, *supra* note 13 at 99–100, 105; Erickson, *supra* note 12 at 419–22. The name dictionary attack originates from using a list of ordinary dictionary words to find a user's password. These types of attacks can be expanded upon by adding common variations of dictionary words (e.g. swapping letters for numbers), combinations of dictionary words, or phrases of particular importance to the targeted user, such as family members' names and birthdates.

52 See Kerr & Schneier, *supra* note 15 at 999.

53 Apple and Android devices are examples of systems that ensure attempts to guess the user's password must be done through the device itself. This is accomplished by combining the user's password with a device-specific key that cannot be extracted, to create the encryption key. See Apple, "iOS Security", *supra* note 36 ("[t]he passcode is entangled with the device's UID, so brute-force attempts must be performed on the device under attack" at 14); William Enck & Adwait Nadkarni, "What if the FBI Tried to Crack an Android Phone? We Attacked One to Find Out", *The Conversation* (29 March 2016), online: <theconversation.com>, archived at https://perma.cc/R7MV-XMVP.

ber of times.[54] This is the feature that initially prevented the FBI from accessing the San Bernardino terrorist's phone.[55]

Police attempts to guess the user's password are therefore constrained by both the complexity of the password and by any countermeasures included in the encryption implementation. As the San Bernardino case demonstrates, even a four-digit numeric pin can pose significant challenges for law enforcement.

II. Legislative Responses

As we have seen, law enforcement's capacity to defeat encryption under current law depends on many variables outside of its control, including: decisions made by the encryption user; the strength and design of the encryption system; and whether users or service providers are willing to cooperate with police. As mentioned, we do not attempt to answer whether this state of affairs is acceptable. Given the increasing power, ubiquity, and security of encryption systems, however, it makes sense to at least consider how government might enhance police access to encrypted data.

There are two main legislative options: (i) requiring service providers to grant police exceptional access to encrypted data through backdoors; and (ii) compelling suspects to decrypt their own information in response to a lawful request enforceable by criminal punishments for noncompliance. In the discussion that follows we evaluate whether either regime is tenable from the perspectives of both policy and constitutional law.

It bears repeating that neither option would imply changing the law regulating the state's entitlement to private information. As the law currently stands, police may use any technical means to decrypt data that they are legally entitled to access. If state agencies obtained a technology capable of quickly and efficiently breaking all current encryption systems, they would be free to use it without restriction. We recognize, and discuss in detail below, that enhancing the state's decryption capacity (whether through legislation or technology) could increase the quantum of private information accessible to police. But it should be kept in mind that while the law gives people the freedom to use encryption and other security measures to protect their data, it has never restricted law enforcement's capacity to defeat those protections.[56]

---

[54] See Kerr & Schneier, *supra* note 15 at 1000.

[55] See *ibid* at 1007; Hack, *supra* note 26 at 8. See also Kim Zetter, "Apple's FBI Battle is Complicated. Here's What's Really Going on", (18 February 2016), *Wired*, online: <https://www.wired.com>, archived at https://perma.cc/TV7K-XU6S.

[56] See the discussion below in Part II.A(2).

A. Exceptional Access

1. Policy

An exceptional access regime would require service providers to build in law-enforcement backdoors for all data encrypted by their systems.[57] It is easy to understand why such a regime would be attractive to law enforcement. In theory, it would give them the ability to easily obtain plaintext for any encrypted information that they are lawfully entitled to access. And, in contrast to the compelled disclosure proposal discussed below, it would provide them with plaintext without any involvement from the user. This would enable the immediate decryption of data acquired through both prospective, surreptitious interception and retrospective seizure from devices used by persons who could not be induced, for whatever reason, to assist with decryption.

Before examining this proposal further, it is important to note that a limited exceptional access regime has existed in Canada since the mid-1990s.[58] As mentioned, where police establish their legal entitlement to information, wireless telecommunications providers must provide it in plaintext form if they have encrypted it.[59] Specifically, the government

---

[57] Exceptional access could be implemented in a number of different ways including: "key escrow" (where service providers would register each encryption key with a third party agent); "golden keys" (where service providers would create a "master key" for unlocking all encrypted data); or, in the case of disk encryption, by requiring service providers to disable the security measures that prevent brute-force attacks. Distinguishing between these exceptional access methods is beyond the scope of this article. For an example of an exceptional access regime, see the draft bill proposed, but not yet introduced, in the United States Senate by Senators Burr and Feinstein, online: <https://www.burr.senate.gov/imo/media/doc/BAG16460.pdf>. See also Rainey Reitman, "Security Win: Burr-Feinstein Proposal Declared 'Dead' for This Year", (27 May 2016), online: Electronic Frontier Foundation <https://www.eff.org/deeplinks/2016/05/win-one-security-burr-feinstein-proposal-declared-dead-year>, archived at https://perma.cc/87HV-9R8H.

[58] See Canada, Library of Parliament Parliamentary Information and Research Service, "Telecommunications and Lawful Access: I The Legislative Situation in Canada" by Dominique Valiquet, Catalogue No PRB 05-65E (Ottawa: Library of Parliament, 21 February 2006) at 4, n 17. See generally Christopher Parsons, "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians" (2015) at 33–39, online: Telecom Transparency Project <www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf>; Parsons & Israel, *supra* note 37.

[59] These standards were initially secret and made public only after reporting. See Colin Freeze & Rita Trichur, "Wireless Firms Agree to Give Ottawa Ability to Monitor Calls, Phone Data", *The Globe and Mail* (16 September 2013), online: <https://www.theglobeandmail.com>, archived at https://perma.cc/QB7Z-SK9A. The government has made several (unsuccessful) attempts to impose similar requirements on all telecom-

has mandated that if providers "initiate encoding, compression or encryption" on communications, they must provide police with the communications "en clair" (i.e. plaintext).[60] This obligation is part of a broader spectrum of licensing conditions requiring providers to enable police access to lawfully acquired telecommunications content and metadata.[61]

This duty to decrypt does not apply, however, to "end to end encryption that can be employed without the service provider's knowledge."[62] This means that wireless telecommunications providers are not obliged to provide plaintext for data that was encrypted, by the user or a third party, before entering the network, even if the provider implemented the encryption system.[63] The duty to decrypt has also been interpreted to apply only to circuit-switched communications such as mobile phone calls, sms text messages, and faxes, and not to packet-switched (i.e. internet) communications.[64]

As a consequence of these exceptions, the duty to decrypt covers only those communications encrypted by telecommunications providers. It does not extend to information encrypted by default on mobile operating systems, such as Apple's iOS and Google's Android. Nor does it apply to communications encrypted end-to-end by application providers, such as WhatsApp, even if they are carried over wireless telecommunications networks. And even if the decryption obligation did apply, the wireless providers subject to the regime would probably not be able to comply. Even in the wireless sphere, therefore, law enforcement's capacity to defeat encryption is limited, and is likely to become increasingly so.

---

munications service providers. See e.g. Bill C-30, *Protecting Children from Internet Predators Act*, 1st Sess, 41st Parl, 2011–2012, cl 6.

60 Public Safety Canada, "Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications: Compliance Table" (17 November 2008) at 6, online: <https://cippic.ca/uploads/Solicitor_General_Standards_Annotaed-2008.pdf>. The accompanying annotation states: "any type of encryption algorithm that is initiated by the service provider must be provided to the law enforcement agency unencrypted." Note that because the government has not made these standards publicly available, there is no way to know whether these standards have since been updated.

61 See Valiquet, *supra* note 58 at 6, n 24.

62 *Ibid* at 6.

63 See Parsons & Israel, *supra* note 37 ("excluded are end-to-end encryption techniques, which may be implemented by the service provider but, once implemented, can be initiated by end users without the knowledge or active participation of that provider").

64 See Parsons, *supra* note 58 at 34.

Not surprisingly, then, police have lobbied for comprehensive exceptional access legislation.[65] As we elaborate below, however, there are significant economic, jurisdictional, and technical hurdles that would have to be overcome to make such a regime a practical reality. More importantly, exceptional access would introduce vulnerabilities into encryption systems that could be exploited by malicious actors.

To begin, any legislation requiring service providers to build in backdoors for police would generate significant upfront development costs. Many technology experts contend that it is simply not possible to design exceptional access in a way that would allow police in while keeping malicious actors, such as criminals and foreign intelligence agencies, out.[66] Even if we assume that this concern is overstated, developing a proposal for secure exceptional access would require extensive research and resources.[67] There would also be significant costs associated with replacing existing encryption systems that do not currently support exceptional access.

Furthermore, the obligations imposed by exceptional access legislation could diminish investment in the Canadian technology sector. As legislation would apply only to providers operating in Canada, many security-conscious users would adopt purely foreign encryption systems.[68] Canadi-

---

65 See e.g. *Green Paper*, *supra* note 1 at 56–57; Canadian Association of Chiefs of Police, "Resolutions Adopted at the 111th Annual Conference" (Ottawa, 2016) at 19–20, online: <www.cacp.ca/index.html?asst_id=1193>, archived at https://perma.cc/B67P-7LWT; Letter from William Fitzpatrick, President, National District Attorneys Association & Terrence M Cunningham, President, International Association of Chiefs of Police, to the Honorable Richard Burr, Chairman, Senate Intelligence Committee & the Honorable Dianne Feinstein, Vice Chairman, Senate Intelligence Committee (13 April 2016), online: <www.theiacp.org/Portals/0/documents/pdfs/NDAA-IACPBurr-FeinsteinEncryption.pdf>.

66 See Abelson et al, *supra* note 7 at 15; Kaye Report, *supra* note 2 at paras 8, 42; Ben Adida et al, "CALEA II: Risks of Wiretap Modifications to Endpoints" (17 May 2013), online: Center for Democracy & Technology <www.cdt.org/files/pdfs/CALEAII-techreport.pdf>; Cook, *supra* note 7; Kalia, *supra* note 39.

67 See Abelson et al, *supra* note 7 at 25; Benjamin Wittes, "Thoughts on Encryption and Going Dark, Part II: The Debate on the Merits" (12 July 2015), *Lawfare* (blog), online: <https://www.lawfareblog.com/thoughts-encryption-and-going-dark-part-ii-debate-merits>, archived at https://perma.cc/8FN2-CTUB.

68 For example, in the aftermath of the Snowden leaks showing the extent of NSA surveillance of major United States-based technology companies, many individuals and organizations adopted foreign technologies offering greater security. And, as discussed, many of the US companies ultimately responded by adopting stronger encryption systems. See "Edward Snowden: Leaks that Exposed US Spy Programme", *BBC News* (17 January 2014), online: <www.bbc.com/news>, archived at https://perma.cc/4DG6-MBU7; van Hoboken & Rubinstein, *supra* note 33 at 508–09. Danielle Kehl et al, "Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity" (July

an operations would become less profitable, and some providers might pull out of Canada altogether rather than bear the burdens of compliance. Smaller start-up firms could also suffer, potentially chilling technological innovation.[69]

The availability of foreign and open-source alternatives would also limit the effectiveness of any exceptional access regime.[70] It would not be difficult for sophisticated users, including ones with malicious intent, to find methods of encrypting information immune to exceptional access.[71] Police would still face situations in which encrypted information is inaccessible to them.

Lastly, and most importantly, exceptional access would expose legitimate, socially-productive uses of encryption to the same vulnerabilities that enable lawful police access. As mentioned, there is an overwhelming consensus among information security experts that exceptional access cannot keep backdoors out of the hands of bad actors.[72] Exceptional access requires some organization to hold the access keys. This is problematic, as a single organization that holds multiple keys presents a concentrated

---

2014) New America's Open Technology Institute Policy Paper at 7–13, online: <www.newamerica.org/downloads/Surveilance_Costs_Final.pdf>.

69 See Abelson et al, *supra* note 7 ("[e]conomic growth comes largely from innovation in science, technology, and business processes. ... Countries that require ... new apps and web services to have their user-to-user communications functions authorized by the government will be at a significant disadvantage" at 17). See also Creig Lamb & Matthew Seddon, *The State of Canada's Tech Sector, 2016* (Toronto: Brookfield Institute for Innovation + Entrepreneurship, 2016) at 4, online: <brookfieldinstitute.ca/wp-content/uploads/2016/08/The-State-of-Canadas-Tech-Sector-2016v2.pdf> (reporting that, in 2016, the technology industry contributed $117 billion (or 7.1%) of Canada's GDP, 61.2% of which was contributed by information and communications technology).

70 See Abelson et al, *supra* note 7 at 18–19; Bruce Schneier, Kathleen Seidel & Saranya Vijayakumar, "A Worldwide Survey of Encryption Products" (11 February 2016) Berkman Center for Internet & Society Research Publication No 2012-2 at 6, online: SSRN <ssrn.com/abstract=2731160>.

71 See Kerr & Schneier, *supra* note 15 at 1012–13.

72 Not all technologists have abandoned hope of creating a secure exceptional access system: see Steven Levy, "Cracking the Crypto War", *Wired* (25 April 2018), online: <https://www.wired.com>, archived at https://perma.cc/H3MP-VLQB (discussing a particular method for implementing exceptional access patented by Ray Ozzie). However, such proposed solutions continue to face significant criticism: see Matthew Green, "A Few Thoughts on Ray Ozzie's 'Clear' Proposal" (26 April 2018), *A Few Thoughts on Cryptographic Engineering* (blog), online: <https://blog.cryptographyengineering.com/2018/04/26/a-few-thoughts-on-ray-ozzies-clear-proposal/>, archived at https://perma.cc/WA3T-EM6R; Bruce Schneier, "Ray Ozzie's Encryption Backdoor" (7 May 2018), *Schneier on Security* (blog), online: <https://www.schneier.com/blog/archives/2018/05/ray_ozzies_encr.html>, archived at https://perma.cc/K9HW-LFXN.

target for attackers seeking to access those keys.[73] And there is also a risk that backdoors will be abused or unintentionally leaked by internal actors.[74]

These risks are not merely hypothetical. From 2004 to 2005, the phone communications of several members of the Greek government were surreptitiously intercepted. This sophisticated attack was carried out by compromising a lawful intercept mechanism built into the telecommunications network.[75] In 2005, Juniper Networks found unauthorized code allowing traffic travelling through its network devices to be decrypted. Some evidence suggests that this code originated as an NSA-requested backdoor.[76] Further, as the Snowden leaks demonstrate, even if backdoors are not penetrated by hackers, they may be disseminated or misused by the people who have access to them.

In summary, policy considerations indicate that exceptional access would be a poor solution to the encryption problem.[77] We do not believe, however, that it would be unconstitutional. While commentators have suggested that it could compromise privacy[78] and free expression,[79] there is little reason to think that it would violate the constitutional provisions protecting these norms: sections 8 and 2(b) of the *Charter*.

---

73 See Abelson et al, *supra* note 7 at 2–3. This holds true whether government, industry, or a trusted third party is vested with the keys to access encrypted information.

74 For example, though it was not part of an exceptional access system, in 2016 Microsoft accidentally disclosed master keys that allowed access to its devices. See Robert Hackett, "Uh-oh! Microsoft Leaks 'Golden Keys' to Windows Devices", *Fortune* (11 August 2016), online: <fortune.com>, archived at https://perma.cc/W545-46UY.

75 See Vassilis Prevelakis & Diomidis Spinellis, "The Athens Affair: How Some Extremely Smart Hackers Pulled off the Most Audacious Cell-Network Break-in Ever", *IEEE Spectrum* (29 June 2007), online: <https://spectrum.ieee.org>, archived at https://perma.cc/TXG8-VDNW.

76 See Steven J Murdoch, "Insecure by Design: Protocols for Encrypted Phone Calls" (2016) 49:3 Computer 25 at 30; Kim Zetter, "Researchers Solve Juniper Backdoor Mystery; Signs Point to NSA", *Wired* (22 December 2015), online: <https://www.wired.com>, archived at https://perma.cc/54F3-AJRX.

77 For a different view, see Eric Manpearl, "Preventing 'Going Dark': A Sober Analysis and Reasonable Solution to Preserve Security in the Encryption Debate" (2017) 28:1 U Fla JL & Pub Pol'y 65.

78 See e.g. A Michael Froomkin, "The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution" (1995) 143:3 U Pa L Rev 709 at 828–30; Anjali Singhal, "The Piracy of Privacy? A Fourth Amendment Analysis of Key Escrow Cryptography" (1996) 7:2 Stan L & Pol'y Rev 189 at 191.

79 See e.g. Kaye Report, *supra* note 2; David B Rivkin Jr & Andrew M Grossman, "Apple, the FBI and Free Speech", *USA Today* (19 February 2016), online: <https://www.usatoday.com>, archived at https://perma.cc/42HD-X6NP.

2. Privacy and Section 8 of the *Charter*

Section 8 states that "[e]veryone has a right to be secure against unreasonable search or seizure." Whether a search or seizure has occurred turns on whether the state has invaded the claimant's "reasonable expectation of privacy."[80] If not, section 8 is not violated. If the state does invade a reasonable expectation of privacy, the court must go to consider whether that invasion was "reasonable".[81]

Any section 8 challenge to exceptional access would very likely fail at the first stage. Put simply, in and of itself, encryption cannot create a reasonable expectation of privacy.[82] As we elaborate in Part II.B(3) below, before they decrypt anyone's data, police must show that they are lawfully entitled to access it. In many cases, the data will be protected by a reasonable expectation of privacy, and police will accordingly have to comply with the requirements of "reasonableness" under section 8 to acquire it. Often, this will require them to get a warrant based on reasonable and probable grounds. But once they have established their entitlement to the data, the law imposes no limits on their efforts to make it intelligible, even if encryption or any other security measure make it difficult to do so.[83]

Consider analog equivalents of encryption. People can lock their private documents in safes or use public pay telephones or anonymous prepaid mobile phones to communicate with others, but if police obtain warrants to seize those documents or communications, they are free to try to overcome those security measures.[84] Imagine that police convince a judge

---

80 See *Hunter v Southam Inc*, [1984] 2 SCR 145 at 159, 11 DLR (4th) 641 [*Hunter*]; *R v Dyment*, [1988] 2 SCR 417 at 426, 73 Nfld & PEIR 13 [*Dyment*].

81 See Penney, Rondinelli & Stribopoulos, *supra* note 28 at 151, 188–91.

82 See Orin S Kerr, "The Fourth Amendment in Cyberspace: Can Encryption Create a 'Reasonable Expectation of Privacy?'" (2001) 33:2 Conn L Rev 503 [Kerr, "Encryption"]. We do not mean to suggest that encryption could never be relevant to whether a reasonable expectation of privacy exists in the first place. A person might be found to have a reasonable expectation of privacy in a computer or device shared with others, for example, in part because he or she has password-protected access to certain files or directories. See *R v Cole*, 2012 SCC 53 at para 56, [2012] 3 SCR 34 [*Cole*]; *R v Craig*, 2016 BCCA 154 at para 104, 335 CCC (3d) 28. Analogously, while placing a garbage bag in a receptacle normally used for collection would ordinarily extinguish any expectation of privacy, locking the receptacle would likely maintain it. See *R v Patrick*, 2009 SCC 17 at para 39, [2009] 1 SCR 579 [*Patrick*].

83 See Kerr, "Encryption", *supra* note 82 ("[w]henever the government obtains ciphertext consistently with Fourth Amendment standards, decrypting the communication into plaintext without a warrant cannot violate the Fourth Amendment" at 505).

84 See generally *Thompson*, *supra* note 21 (authorizations to intercept calls from public payphones).

that a residence likely contains documents relevant to the investigation of an offence and obtain a warrant to search that residence for those documents. As the documents may exist in either paper or digital form, the warrant specifically authorizes both physical and computer searches.[85] Police enter the residence and find a locked filing cabinet, shredded papers in a garbage bin, a letter with seemingly illegible handwriting, a sheet of paper with coded message written on it, and a computer locked with a password. The law unquestionably permits them to break the lock on the cabinet, put the shredded papers back together, analyze the messy handwriting, and decipher the coded text. There is no reason why they should not also be able to defeat the computer's password protection.[86] As the Supreme Court has held, the vast storage and connective capacities of digital devices raise unique concerns about overbroad searches and the potential need for minimizing search protocols.[87] But none of these concerns relate to encryption. Even if the warrant specified that police could search the computer only for a highly specific file type, created in narrowly limited time frame, and located in a directory connected to a single user's profile, they would surely be entitled to decrypt those files.

Nothing in search and seizure jurisprudence detracts from this conclusion. Police are permitted to use destructive methods, for example, to gain access to secured or hidden evidence, so long as the methods used are reasonable in the circumstances.[88] Courts have also held that people cannot create a reasonable expectation of privacy by selectively excluding police from premises generally open to the public.[89] And the Supreme Court emphasized in *Fearon* that the presence or absence of password security

---

85 See *R v Vu*, 2013 SCC 60 at paras 46–48, [2013] 3 SCR 657 [*Vu*] (police executing search warrants cannot search computers without specific judicial preauthorization).

86 See Kerr, "Encryption", *supra* note 81 at 513–20.

87 See *Vu*, *supra* note 85 at paras 25, 53–62 (search protocols and other minimizing conditions are not generally required for computer searches under s 8 but may be imposed on a case-by-case basis). See also *R v Morelli*, 2010 SCC 8 at paras 2–3, 105, [2010] 1 SCR 253; *R v Fearon*, 2014 SCC 77 at paras 51–52, [2014] 3 SCR 621 [*Fearon*]; *Cole*, *supra* note 82 at para 47; *R v Spencer*, 2014 SCC 43 at para 46, [2014] 2 SCR 212 [*Spencer* 2014].

88 See e.g. *R v Sekhon*, 2009 BCCA 187 at paras 83–91, 189 CRR (2d) 176 (customs officials reasonably drilled into a truck bed to find secret compartment holding drugs); *R v Hardy* (1995), 103 CCC (3d) 289 at 300–02, 66 BCAC 270, (the drilling of a suitcase liner by customs officials was reasonable).

89 See *R v Felger*, 2014 BCCA 34, 306 CCC (3d) 143, leave to appeal to SCC refused, 35795 (17 October 2014) (no reasonable expectation of privacy was breached when undercover police entered a store where a "No Police" sign was posted).

on mobile phones does not determine whether they attract a reasonable expectation of privacy.[90]

The issue in *Fearon* was whether police need a warrant to search mobile devices seized as an incident of arrest. The majority held that, subject to certain limitations, they do not. The dissenting justices would have found that warrants are required, save for exigent circumstances. Notwithstanding this division, the Court unanimously concluded that mobile devices attract a reasonable expectation of privacy and, most importantly for our purposes, that the failure to use a password does not extinguish that expectation.[91] It seems to us that the converse should also be true: a password cannot create a reasonable expectation of privacy.[92] Therefore, if police have "reasonably" invaded the user's expectation of privacy in the device, they are entitled to try to defeat any passwords or encryption protecting it.

In her dissenting reasons, which advocated for the more privacy-protective outcome, Justice Karakatsanis specifically referred to the difficulties that police may have in accessing encrypted devices, asserting that this did not detract from the necessity of preauthorization.[93] This approach is inconsistent with the notion that encryption can create a legal barrier to police access. Though the specific question was not before the Court, Justice Karakatsanis clearly assumed that police would be entitled to defeat encryption after they obtained a warrant to search the device.

Of course, the jurisprudence reviewed above relates to state access to potentially encrypted data in individual search and seizure cases. Those objecting to exceptional access on privacy grounds often claim that by potentially making more personal data accessible to police, backdoors would significantly erode individual privacy in the aggregate.[94] They may have a point. But it does not necessarily follow that this would be a negative out-

---

90 *Supra* note 87 at para 53.

91 *Ibid* ("[a]n individual's decision not to password protect his or her cell phone does not indicate any sort of abandonment of the significant privacy interests one generally will have in the contents of the phone" at para 53). In her dissent, Karakatsanis J, agreed on this point ("[l]eaving a cell phone without password protection cannot be said to constitute a waiver of the privacy interest in the vast web of digital information accessible through the phone, nor does it demonstrate a subjectively diminished expectation of privacy" at para 160). See also *R v Marakah*, 2017 SCC 59 at para 106, [2017] SCJ No 59 (QL), Moldaver J, dissenting.

92 *Fearon*, *supra* note 87 ("I would not give this factor [whether the phone is password-protected] very much weight in assessing either an individual's subjective expectation of privacy or whether that expectation is reasonable" at para 53).

93 *Ibid* at para 148, Karakatsanis J, dissenting.

94 See e.g. Froomkin, *supra* note 78 at 840.

come. First, law enforcement agencies have argued forcefully that strong and ubiquitous encryption has diminished, or threatens to diminish, the net availability of evidence as compared to the analog era.[95] On this view, exceptional access would merely restore the previous privacy-security balance.

Secondly, even if exceptional access would give police more access to personal information than before, this would not necessarily be objectionable. The privacy-security trade-off is not always a zero sum game.[96] If police usually require warrants to obtain encrypted data, exceptional access could increase the amount of forensically relevant information without dramatically increasing the frequency of privacy invasions of the innocent.[97] If a technology can substantially enhance law enforcement's capacity to detect and deter wrongdoing without substantially impinging on the liberties of law-abiding citizens, why shouldn't the law permit it?

We need not definitively resolve this debate here, however. It should suffice to say that deciding whether exceptional access would unduly diminish aggregate privacy entails enormously difficult empirical and normative questions, questions that are better suited to informed, democratic deliberations by Parliament than to case-by-case adjudication by the courts.[98] Parliament's capacity to gather expert information, gauge public preferences, and craft detailed regulations applying to a broad range of circumstances far exceeds that of the courts.[99] And as the failure of many attempts to adopt modern "lawful access" legislation has shown, the internet privacy lobby is strong and effective.[100] There is no evidence of any

---

95 See *Green Paper*, *supra* note 1 at 60–65; Canada, Department of Justice, "Summary of Submissions to the Lawful Access Consultation" (28 April 28 2003) at 10, online: <www.justice.gc.ca/eng/cons/la-al/sum-res/sum-res.pdf>; Susan Landau, *Surveillance or Security?: The Risks Posed by New Wiretapping Technologies* (Cambridge, Mass: MIT Press, 2010) at 7.

96 See Ric Simmons, "Ending the Zero-Sum Game: How to Increase the Productivity of the Fourth Amendment" (2013) 36:2 Harv JL & Pub Pol'y 549.

97 See generally Steven Penney, "Unreasonable Search and Seizure and Section 8 of the *Charter*: Cost-benefit Analysis in Constitutional Interpretation" in Errol Mendes & Stéphane Beaulac, eds, *Canadian Charter of Rights and Freedoms*, 5th ed (Markham: LexisNexis, 2013) 751 at 775–78 [Penney, "Cost-Benefit Analysis"].

98 *Ibid* at 757–60.

99 *Ibid*. See also James Stribopoulos, "In *Search* of Dialogue: The Supreme Court, Police Powers and the *Charter*" (2005) 31:1 Queen's LJ 1 at 61–73.

100 See e.g. Jesse Brown, "Slacktivism Defeats Lawful Access", *Maclean's* (21 September 2011), online: <www.macleans.ca>, archived at https://perma.cc/3QP7-3Y5E (detailing the influence of a 70,000-person petition opposing the proposed legislation); Michael Geist, "Ottawa Finds Public No Pushover on Snooping Law", *Toronto Star* (30 October 2006) E3. For examples of a similar phenomenon in the United States, see e.g. Orin S Kerr, "The Fourth Amendment and New Technologies: Constitutional Myths and the

democratic deficit that might justify counter-majoritarian intervention by the judiciary.[101]

Lastly, even if courts held that exceptional access invaded a reasonable expectation of privacy, claimants would still have to establish that the invasion was unreasonable. But what would a "reasonable" exceptional access regime entail? The usual requirements of preauthorization on reasonable and probable grounds are irrelevant. In most cases police would have already satisfied them in demonstrating their lawful entitlement to the data; and where the law permits access on other grounds, what other decryption-related conditions would apply? Surely section 8 does not prohibit exceptional access altogether? If it did, the wireless carrier exceptional access regime in place since the 1990s would be unconstitutional, which no court has found. And if it does not, on what basis would a court decide that some regimes are permissible and some not? The purpose of exceptional access is to prevent digital evidence from "going dark" *vis-à-vis* law enforcement. If courts were to gauge a regime's reasonableness on the extent it permits users to exempt their data from its scope, that purpose would be almost wholly defeated. Criminal and other malicious actors would have a much stronger incentive to exploit gaps in coverage than law-abiding users. And providers would likely face consumer and competitive pressure to use exempt forms of encryption.

In summary, section 8 of the *Charter* does not provide a suitable framework for deciding whether exceptional access unduly threatens privacy. While exceptional access does raise privacy concerns, these pale in comparison to the security and economic risks discussed in Part II.A(1), above. In any case, Parliament is well placed to address the privacy impacts of exceptional access regimes, should it (unwisely) seek to implement one.

3. Freedom of Expression and Section 2(b) of the *Charter*

Section 2(b) of the *Charter* states that everyone is entitled to the fundamental freedoms of "thought, belief, opinion and expression, including freedom of the press and other media of communication." The section 2(b) guarantee is violated when the state, in purpose or effect, restricts a per-

---

Case for Caution" (2004) 102:5 Mich L Rev 801 at 839–58, 881–82; Craig S Lerner, "Legislators as the 'American Criminal Class': Why Congress (Sometimes) Protects the Rights of Defendants" [2004] 3 U Ill L Rev 599 at 621–22.

[101] See generally John Hart Ely, *Democracy and Distrust: A Theory of Judicial Review* (Cambridge, Mass: Harvard University Press, 1980) at 96–97.

son's ability to carry out expressive activities conveying meaning.[102] The provision also prevents the state from compelling persons to express themselves.[103]

Free expression-based challenges to exceptional access have been framed in two ways. The first is that computer code is expressive, and that requiring coding to implement backdoors violates the prohibition against compelled expression.[104] Second, some contend that by limiting people's ability to communicate securely, backdoors infringe freedom of expression for encryption users generally.[105] In our view, neither argument is viable under section 2(b).

The first claim founders on the fact that the coding of backdoors is not expressive. Like human speech, computer code can be expressive in some contexts and purely functional in others.[106] Consider a vehicle capable of setting its speed in response to voice commands. The use of speech to adjust the vehicle's speed is functional—it has no expressive character. Similarly, whether computer code is expressive or not depends on the context. Where coding produces an expressive outcome, such as website content or a video game, that outcome is protected by section 2(b).[107] In contrast, requiring an encryption provider to implement a backdoor is no different than requiring a manufacturer to comply with safety standards in designing a product.[108] While exceptional access would compel service providers to produce computer code, it would not compel expression.

---

102 See *Irwin Toy Ltd v Quebec (AG)*, [1989] 1 SCR 927 at 971–72, 58 DLR (4th) 577 [*Irwin Toy*].

103 See *Slaight Communications Inc v Davidson*, [1989] 1 SCR 1038, 59 DLR (4th) 416 [cited to SCR] ("freedom of expression necessarily entails the right to say nothing or the right not to say certain things" at 1080).

104 This was one of the arguments advanced by Apple in response to the FBI's request to access the iPhone implicated in the San Bernardino terrorist attack. See Laura Sydell, "In Fighting FBI, Apple Says Free Speech Rights Mean No Forced Coding", *National Public Radio* (27 February 2016), online: <https://www.npr.org>, archived at https://perma.cc/WB7Y-SSLU. See also Alex Colangelo & Alana Maurushat, "Exploring the Limits of Computer Code as a Protected Form of Expression: A Suggested Approach to Encryption, Computer Viruses, and Technological Protection Measures" (2006) 51:1 McGill LJ 47 at 59–60.

105 See Kaye Report, *supra* note 2 at para 43.

106 See Veenu Goswami, "Algorithms, Expression, and the *Charter*: A Way Forward for Canadian Courts" (2017) 7:1 Western J Leg Studies 1 at 4–5; Neil Richards, "Apple's 'Code = Speech' Mistake", *MIT Technology Review* (1 March 2016), online: <https://www.technologyreview.com>, archived at https://perma.cc/V8U5-SGE9.

107 See generally *Irwin Toy*, *supra* note 102 at 968–71.

108 Some have argued that exceptional access differs from product regulation because encryption providers may need to use a digital signature to implement backdoors,

The second argument—that exceptional access would restrict free expression for encryption users generally—reflects one of the policy concerns discussed above, i.e. that backdoors would compromise data security and consequently deter people from engaging in expressive communications and activities online. While this is a legitimate issue for Parliament to consider, the effect of exceptional access on freedom of expression is at best uncertain. Like other *Charter* rights, section 2(b) only protects individuals against state-imposed limitations on the implicated right or freedom.[109] Exceptional access does not empower the state to impose any sanctions or restrictions on speech. The most that can be said is that it could deter expression by those who fear that their communications could be decrypted and used for improper purposes by state or non-state actors. But given that non-regulated encryption technologies would still exist, as discussed above, it would be difficult to show that an exceptional access law dissuaded anyone concerned about this risk from expressing themselves. Though the Supreme Court has held that indirect chilling effects on expression can be inferred in obvious cases, there must be a causal connection between the impugned law and the exercise of the section 2(b) right.[110] The effect of exceptional access on encryption users' freedom of expression is too remote and speculative to ground a section 2(b) claim.

B. Compelled Disclosure

1. Policy

Unlike exceptional access, a compelled disclosure regime would not require encryption providers to give law enforcement backdoor access to encrypted data. Instead, it would require encryption *users* to either hand over their keys or provide plaintext when police have independently es-

---

amounting to a compelled endorsement of encryption policy. See Andrew Crocker, "What We Talk About When We Talk About Apple and Compelled Speech" (8 March 2016), online: Electronic Frontier Foundation <https://www.eff.org/deeplinks/2016/03/what-we-talk-about-when-we-talk-about-apple-and-compelled-speech>, archived at https://perma.cc/3JLH-5VE3. This argument is flawed in two respects. First, digital signatures serve a functional purpose: they are used to verify the authenticity of computer code as a security measure. Comparing their use to a political endorsement grossly overstates their purpose. Second, even if digital signatures were expressive in nature, these requirements are built into systems by the provider. It would be counterintuitive to allow companies to avoid complying with the law simply because they have developed obstacles that can only be disabled through an expressive act.

109 See *Irwin Toy*, *supra* note 102 at 967–68.

110 See *R v Khawaja*, 2012 SCC 69 at paras 79–84, [2012] 3 SCR 555.

tablished lawful authority to access the data.[111] If they fail to do so, users could be charged with an offence and face penal sanctions, such as imprisonment.[112]

On the one hand, compelled disclosure is a less comprehensive solution to the encryption problem than exceptional access. It would not allow police to decrypt surveillance intercepts in real time. Nor would it enable decryption in any case where the user was unidentified, deceased, incapacitated, at large, or otherwise unable or unwilling to provide the key. Sophisticated users might also be able to adopt countermeasures to either prevent encrypted data from being discovered on seized devices or make it difficult to prove that they possessed the key.[113]

On the other hand, compelled disclosure avoids many of the problems associated with exceptional access. It creates no security vulnerabilities; imposes no economic burden on industry, consumers, or police; and can be enforced without jurisdictional constraint. It thus promises to provide police with lawful access to a significantly greater quantum of encrypted data than is possible under current law. Further, in comparison to exceptional access, it also greatly minimizes the risk that law enforcement or national security agencies will engage in illegal, abusive, or discriminatory surveillance.[114] As detailed in Part II.B(2) below, to cohere with section 8 of the *Charter*, any compelled disclosure regime would presumptively require police to obtain a warrant based on probable grounds to believe that the suspect had the capacity to decrypt data that police were legally entitled to access.

---

[111] This type of regime has been adopted in several jurisdictions, including the United Kingdom: *Regulation of Investigatory Powers Act 2000* (UK), c 23, ss 49–56 [*RIPA*]; and the commonwealth (federal) jurisdiction in Australia: *Crimes Act 1914* (Cth), s 3LA [*Crimes Act*].

[112] See *RIPA*, *supra* note 111, s 53 (making it an offence to "knowingly" fail to disclose after being given notice, subject to a two year maximum jail term or fine); *Crimes Act*, *supra* note 111, s 3LA(5) (two year maximum for failing to comply with disclosure order).

[113] See Timothy A Wiseman, "Encryption, Forced Decryption, and the Constitution" (2015) 11:2 I/S: J L & Policy Information Society 525 at 568–74; Alexei Czeskis et al, "Defeating Encrypted and Deniable File Systems: TrueCrypt v5.1a and the Case of the Tattling OS and Applications" (Paper delivered at the 3rd Usenix Workshop on Hot Topics in Security, 2008), online: <https://www.usenix.org/legacy/event/hotsec08/tech/full_papers/czeskis/czeskis.pdf>; Maged H Ibrahim, "Receiver-deniable Public-Key Encryption" (2009) 8:2 Intl J Network Security 159.

[114] It could also reduce police reliance on the types of lawful, but nevertheless highly intrusive, methods of defeated encryption discussed in Part II, above. See *R v Fitzpatrick*, [1995] 4 SCR 154 at paras 47–48, 129 DLR (4th) 129 [*Fitzpatrick*] (noting that if mandatory self-reporting of fish catches were inadmissible in prosecutions, regulators would be forced to use more intrusive and expensive techniques to acquire evidence of wrongdoing).

Some have nonetheless objected to compelled disclosure on self-incrimination and privacy grounds.[115] As these interests are recognized in the jurisprudence interpreting sections 7 and 8 of the *Charter*, respectively, it makes sense to canvass these objections in the context of that case law. In brief, we argue that with appropriate limitations, compelled disclosure would not unduly compromise self-incrimination or privacy and should be upheld under the *Charter*.

2. Self-Incrimination and Section 7 of the *Charter*

Protection against self-incrimination is provided by sections 7, 11(c), and 13 of the *Charter*. Sections 11(c) and 13 provide such protection explicitly,[116] but only in the context of formal legal proceedings as they do not apply to the investigative stage of the criminal process.[117] The Supreme Court of Canada has read section 7, however, to protect against compelled self-incrimination outside of formal proceedings in some circumstances.[118] Section 7, which gives everyone the right not to be deprived of "life, liberty and security of the person ... except in accordance with the principles of fundamental justice," does not speak of self-incrimination. But the Court has recognized the "self-incrimination principle" as a principle of fundamental justice and provided a framework for

---

[115] See Canadian Civil Liberties Association, "Canadians Have Legal Right not to Surrender Their Passwords" (30 August 2016), online: <https://ccla.org/canadians-legal-right-not-surrender-passwords>, archived at https://perma.cc/RV9P-EDPF; N Dalla Guarda, "Digital Encryption and the Freedom from Self-Incrimination: Implications for the Future of Canadian Criminal Investigations and Prosecutions" (2014) 61:1 Crim LQ 119 at 135–36.

[116] S 11(c) guarantees the right of a person "charged with an offence" to "not to be compelled to be a witness in proceedings against that person in respect of the offence." Briefly stated, it prohibits the Crown from compelling defendants to testify in criminal and regulatory prosecutions. S 13 protects the right of a "witness who testifies in any proceedings" to not "have any incriminating evidence so given used to incriminate that witness in any other proceedings, except in a prosecution for perjury or for the giving of contradictory evidence." This provision prevents the Crown from adducing testimony given by defendants in previous proceedings when they were compellable witnesses, if that testimony would incriminate them at their own trial. See David M Paciocco & Lee Stuesser, *The Law of Evidence*, 7th ed (Toronto: Irwin Law, 2015) at 310.

[117] See *Federation of Law Societies of Canada v Canada (AG)*, 2013 BCCA 147 at para 98, 359 DLR (4th) 1, rev'd on other grounds, 2015 SCC 7, [2015] 1 SCR 401; *Fitzpatrick*, *supra* note 114 at para 19. This is true as well of the *Canada Evidence Act*, RSC 1985, c C-5, s 5(2), which provides use immunity to self-incrimination in federal proceedings to those who invoke its protection. See generally David M Paciocco, *Charter Principles and Proof in Criminal Cases* (Toronto: Carswell, 1987) at 465–66, 485–89; Sidney N Lederman, Alan W Bryant & Michelle K Fuerst, *Sopinka, Lederman & Bryant: The Law of Evidence in Canada*, 4th ed (Markham: LexisNexis, 2014) at 524–25.

[118] See Paciocco & Stuesser, *supra* note 116 at 365–72.

deciding whether pretrial compulsion violates it.[119] The principle is not a "free-standing legal protection," however.[120] Even if the state compels a person to self-incriminate, courts will only grant protection after a flexible and pragmatic balancing of interests, including the importance of admitting relevant evidence to determine the truth.[121]

The first question is whether compelled decryption engages any self-incrimination interests. Non-testimonial evidence, such as evidence obtained outside of formal proceedings, may be grouped into two categories: linguistic (or communicative) and non-linguistic (or non-communicative).[122] Linguistic evidence includes documents and statements.[123] Non-linguistic evidence includes bodily samples, bodily impressions, and participation in identification lineups.[124] When the state compels linguistic evidence, the self-incrimination principle is clearly engaged and, depending on a balancing of interests, section 7 may be violated.[125] Self-incrimination is not as obviously implicated by the compulsion of non-linguistic evidence.

Before the *Charter*, courts rejected claims that compelled takings of non-linguistic evidence violated either common law or statutory protections against self-incrimination.[126] This position has shifted under the *Charter*, but only nominally. The Supreme Court has stated that non-

---

[119] See Paciocco & Stuesser, *supra* note 116 at 368–69; Penney, Rondinelli & Stribopoulos, *supra* note 28 at 370–76; *R v White*, [1999] 2 SCR 417 at para 45, 174 DLR (4th) 111 [*White*].

[120] *R v Hart*, 2014 SCC 52 at para 123, [2014] 2 SCR 544 [*Hart*]. See also *R v S (RJ)*, [1995] 1 SCR 451, 121 DLR (4th) 589 [*S (RJ)*] ("the principle against self-incrimination may mean different things at different times and in different contexts" at para 107); *R v SAB*, 2003 SCC 60, [2003] 2 SCR 678 [*SAB*] (noting that "the principle is "not absolute" at para 34).

[121] See *Fitzpatrick*, *supra* note 114 at paras 25–30; *White*, *supra* note 119 at paras 47–48; *R v D'Amour (M)* (2002), 163 OAC 164 at para 47, 166 CCC (3d) 477 [*D'Amour*].

[122] See Steven Penney, "What's Wrong with Self-Incrimination? The Wayward Path of Self-Incrimination in the Post-*Charter* Era: Part III: Compelled Communications, the Admissibility of Defendants' Previous Testimony, and Inferences from Defendants' Silence" (2004) 48:4 Crim LQ 474 at 504 [Penney, "Self-Incrimination, Part III"].

[123] *Ibid*.

[124] *Ibid*.

[125] See *Fitzpatrick*, *supra* note 114 at paras 19, 27–28; *White*, *supra* note 119 at paras 37–48; *R v Jones*, [1994] 2 SCR 229 at 248–49, 114 DLR (4th) 645 [*Jones*].

[126] See *Quebec (AG) v Begin*, [1955] SCR 593, [1955] 5 DLR 394 (blood sample); *Curr v R*, [1972] SCR 889, 26 DLR (3d) 603 (breath sample); *Marcoulx v R*, [1976] 1 SCR 763 at 767–69, 60 DLR (3d) 119 (identification lineup).

linguistic compulsion can be self-incriminating.[127] The Court, however, has preferred to assess its constitutionality under section 8, considering the usual suite of factors inhering in the privacy versus law enforcement calculus.[128]

It is important to decide, therefore, whether compelled decryption should be characterized as linguistic or non-linguistic. If it is the former, self-incrimination concerns are fully engaged; if the latter, the focus should be on whether compelled decryption constitutes an unreasonable search or seizure under section 8 of the *Charter*.

While compelled decryption has attributes of both linguistic and non-linguistic compulsion, in our view it mostly non-linguistic. It is linguistic in that it compels users to disclose that they possess the key or password to the device or that their biometric features are linked to it.[129] It can of-

---

[127] See *R v Stillman*, [1997] 1 SCR 607 at paras 83–86, 144 DLR (4th) 193 [*Stillman*]; *SAB*, *supra* note 120 at paras 34–35; *R v Nedelcu*, 2012 SCC 59 at para 75, [2012] 3 SCR 311 [*Nedelcu*].

[128] See *SAB*, *supra* note 120 ("the principles of fundamental justice that are alleged to be implicated by a DNA search and seizure, including the principle against self-incrimination, are more appropriately considered under a s 8 analysis" at para 35); *R v Grant*, 2009 SCC 32, [2009] 2 SCR 353 [*Grant*] ("the *Charter* concerns raised by the gathering of non-testimonial evidence are better addressed by reference to the interests of privacy, bodily integrity and human dignity, than ... by analogy to compelled statements" at para 104). See also Lee Stuesser, "*R v SAB*: Putting 'Self-Incrimination' in Context" (2004) 42:2 Alta L Rev 543 at 543; *R v Beare; R v Higgins*, [1988] 2 SCR 387, 55 DLR (4th) 481 [*Beare*] (upholding mandatory fingerprinting of arrestees under s 7 without mentioning self-incrimination); *R v Thomsen*, [1988] 1 SCR 640, 40 CCC (3d) 411 (rejecting *Charter* challenges to compelling of bodily samples for alcohol analysis in impaired driving context without mentioning self-incrimination); *R v Bernshaw*, [1995] 1 SCR 254 at para 51, [1995] 3 WWR 457 (noting that compelling of breath samples for alcohol analysis requires reasonable and probable grounds under s 8, with no mention of self-incrimination).

The strongest assertion of the view that compelling non-linguistic evidence implicates self-incrimination is in the Supreme Court's decision in *Stillman*, *supra* note 127 at paras 80–98, in the context of deciding whether to exclude unconstitutionally obtained evidence under s 24(2) of the *Charter*. The Court expressly repudiated this aspect of *Stillman* in *Grant*, *supra* note 128 at paras 65, 100–07. See also David M Paciocco, "*Stillman*, Disproportion and the Fair Trial Dichotomy under Section 24(2)" (1997) 2 Can Crim L Rev 163 ("in equating intimate bodily substances with testimony we are not so much reacting to the compelled participation of the accused as we are to the violation of the privacy and dignity of the person that obtaining such evidence involves" at 170, quoted with approval in *Grant*, *supra* note 128 at para 105).

[129] See generally *Boudreau-Fontaine*, *supra* note 8 at paras 39–44. In that case, police obtained a search warrant including a provision purporting to compel an arrestee to provide his device password. While the court viewed this as improper self-incrimination, it did not conduct any s 7 self-incrimination analysis. The decision therefore stands only for the proposition that there was no legal authorization for the provision and it accordingly violated s 8 of the *Charter* (*ibid* at paras 45–46).

ten be inferred from this information that the user had access to the encrypted device and is aware of its contents.

But the encryption key itself should be viewed as non-linguistic compulsion. Like all digital data, it does communicate information. But it does so in a manner categorically different from the kinds of linguistic acts traditionally enjoying self-incrimination protection.[130] Though encryption keys are, like language, expressed in alphanumeric form, unlike language they serve a purely mechanistic purpose.[131] Moreover, unlike language, they do not convey information about the material world or the user's experience of it; they merely unlock the security feature that prevents communicative content from being understood.[132] As Reitinger puts it, while a

---

[130] See Terzian, *supra* note 3 at 1134–35.

[131] Indeed, in some encryption systems the sole purpose of the user's selected password is to protect a much longer, computer generated password that is used for the actual encryption. Similarly, passwords can effectively be compelled without users revealing them to police, such as when they enter the password on a device themselves to enable access. In neither case does it make much sense to say that users have been forced to reveal a product of their mind or will. See Wiseman, *supra* note 113 at 553, 562.

[132] See *R v S and another*, [2008] EWCA Crim 2177 at para 21, [2009] 1 All ER 716 [*R v S*]; Phillip R Reitinger, "Compelled Production of Plaintext and Keys" [1996] U Chicago Legal F 171 at 174–75, 196; Terzian, *supra* note 3 at 1136.

The American jurisprudence on this point is complex and inconsistent. Most courts have held that the Fifth Amendment's self-incrimination clause forbids the compulsion of passwords but permits compelling biometric information. Compelling the production of plaintext may also be permissible, with some courts requiring the government to establish its prior knowledge of the encrypted contents with "reasonable particularity": see e.g. *In Re Grand Jury Subpoena Duces Tecum*, 670 F (3d) 1335 (11th Cir 2012). In other cases, courts have simply required proof that the suspect had the ability to decrypt: see e.g. *United States v Spencer*, 2018 WL 1964588 (ND Cal 2018); *United States v Apple MacPro Computer*, 851 F (3d) 238 (3d Cir 2017). See also Richard M Thompson II & Chris Jaikaran, "Encryption: Selected Legal Issues", Congressional Research Service, Catalogue No 7–5700 (3 March 2016) at 6–16; Wiseman, *supra* note 113 at 538–52; Aloni Cohen & Sunoo Park, "Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries" (2018) [draft manuscript] online, SSRN: <https://ssrn.com/abstract=3117984>; Laurent Sacharoff, "Unlocking the Fifth Amendment: Passwords and Encrypted Devices" (2018) 87:1 Fordham L Rev 203. But see *In the Matter of a Grand Jury Investigation*, 88 NE (3d) 1178 (Mass App Ct 2017), leave to appeal to Mass SJC denied, 478 Mass 1109 (2018) (no Fifth Amendment violation where a court ordered the petitioner to provide a password where the state established his ownership and control of the device).

As discussed in the text below, distinguishing between these forms of decryption makes little sense in policy terms. Given this, as well as the Fifth Amendment's unique textual and interpretive context, it is doubtful whether the American approach to the issue is of much use in the Canadian context. See also Terzian, *supra* note 3 at 1135–36 (criticizing decisions forbidding compelled decryption as misreading of Fifth Amendment jurisprudence); Orin S Kerr "Compelled Decryption and the Privilege Against Self-incrimination", Tex L Rev [forthcoming in 2018], online: https://ssrn.com/abstract=

key "might arguably have content, albeit arbitrary content, it has no necessary meaning."[133] And while passwords and encryption keys may originate or reside in the user's mind, they also have an independent, material existence analogous to a physical key.[134]

This situation is analogous to one considered in *R. v. Orbanski*, where the accused argued that requiring motorists to perform physical sobriety tests violated the self-incrimination principle.[135] The Supreme Court suggested that admitting evidence of such tests to prove impairment would likely violate the principle. But using the tests to give police grounds to make a breath sample demand would not, even though the laboratory analysis of the sample could be used to prove impairment.[136] In other words, though compelling the suspect's participation in creating new communicative evidence ("my bodily movements indicate I am probably drunk") caused self-incrimination, using that evidence to make pre-existing physical evidence (bodily samples) available to the state to prove the offence did not. Compelling decryption similarly creates new, communicative, self-incriminating evidence ("my ability to decrypt shows my connection to the data"), but the use of that evidence to make pre-existing physical evidence (the plaintext data) available to the state to prove the offence does not.

This distinction can be further illustrated by comparing the different ways that users could be compelled to decrypt. As mentioned, giving an alphanumeric password to police appears plainly linguistic and communicative. But other methods of achieving the same goal do not. Instead of compelling passwords, for example, the law could require suspects to provide encrypted data in intelligible form.[137] In this scenario, suspects are not required to disclose any communicative content that did not exist independent of the compulsion, beyond the implied statement that they can

---

3248286 (arguing that compelled decryption does not violate the Fifth Amendment when the government can show that the user knows the password).

133 Reitinger, *supra* note 132 at 175.

134 See *R v S*, *supra* note 132 at paras 15–16, 20–21 (upholding the compelled decryption provisions of *RIPA*, *supra* note 111, under the *Convention for the Protection of Human Rights and Fundamental Freedoms*, 4 November 1950, 213 UNTS, art 6 (entered into force 3 September 1953)).

135 *R v Orbanski; R v Elias*, 2005 SCC 37, [2005] 2 SCR 3.

136 *Ibid* at paras 58–59. See also *R v Milne* (1996), 28 OR (3d) 577, 107 CCC (3d) 118 (CA); *R v Coutts* (1999), 45 OR (3d) 288 at paras 15–18, 136 CCC (3d) 225 (CA); *R v Visser*, 2013 BCCA 393 at paras 62–72, 342 BCAC 129; *R v Rivera*, 2011 ONCA 225 at para 48ff, 83 CR (6th) 66.

137 See *RIPA*, *supra* note 111, s 50(1)(b).

decrypt the data.[138] As the Supreme Court has held, the self-incrimination principle applies only to material "brought into existence by the exercise of compulsion by the state."[139] Similarly, where the encrypted data is protected by biometric security, compelling users to provide the required biometric produces no linguistic or communicative content, beyond the implied statement described above.

It is difficult to fathom how the law could rationally differentiate between these scenarios. In each case, the nature of the compulsion ("assist in decrypting your information or be punished") and the information revealed (plaintext and an admission of a capacity to decrypt) is the same. And since Canadian law treats analogous situations, such as the compelling of bodily samples and pre-existing documents, as implicating primarily privacy concerns, and only nominally as self-incrimination concerns, it should do the same for encryption keys, no matter what the method of inducing them. Viewed in this way, the only truly linguistic aspect of compelled decryption is the implied statement "I am able to decrypt the data" and its concomitant inferences.[140] The section 7 *Charter* analysis should be conducted with this in mind.

That analysis consists of two steps. In the first, claimants must establish that the type of compulsion at issue would compromise the purposes underlying the principle against self-incrimination.[141] If they are successful, the court must provide one of two remedies. In most cases, it will permit the compulsion, but grant use and derivative use immunity to any evidence obtained from it.[142] Alternatively, in rare instances, the compulsion may be barred altogether. We expand on each of these analytical steps below.

---

[138] See *R v S*, *supra* note 132 ("[i]n much the same way that a blood or urine sample provided by a car driver is a fact independent of the driver, which may or may not reveal that his alcohol level exceeds the permitted maximum, whether the appellants' computers contain incriminating material or not, the keys to them are and remain an independent fact" at para 21).

[139] *British Columbia Securities Commission v Branch*, [1995] 2 SCR 3 at para 43, 123 DLR (4th) 462 [*Branch*]. See also *R v Porter*, 2015 ABCA 279 at para 21, 607 AR 38; *D'Amour*, *supra* note 121 at paras 37–43.

[140] See *R v S*, *supra* note 132 at para 24.

[141] See *Fitzpatrick*, *supra* note 114 at paras 43–48.

[142] Derivative use immunity prevents authorities from admitting evidence "which could not have been obtained, or the significance of which could not have been appreciated, but for the [compelled] testimony of a witness": *S (RJ)*, *supra* note 120 at para 191. See also *Thomson Newspapers Ltd v Canada (Director of Investigation and Research, Restrictive Trade Practices Commission)*, [1990] 1 SCR 425 at 560–61, 67 DLR (4th) 161 [*Thomson Newspapers*].

According to the Supreme Court, the principle against self-incrimination has two rationales: "to protect against unreliable confessions, and to protect against abuses of power by the state."[143] In *Fitzpatrick*, it outlined four factors to be considered in deciding whether statutory compulsion conflicts with the principle: the existence of coercion, the existence of an adversarial relationship, the risk of unreliable confessions, and the risk of abuses of state power.[144]

Where individuals are compelled to assist with decryption, coercion is imposed by the threat of penal consequences. For self-incrimination purposes, however, the coercion relates only to suspects' forced acknowledgment that they possess the key. No self-incrimination arises from any coercion associated with state's acquisition of the encrypted data itself. Though that data may have been obtained coercively (e.g. by taking personal information or property without consent), the coercion is justified if police adhered to the limitations of a constitutionally valid search power.[145] As discussed below in Part II.B(3), whether they did or did not is a question to be answered under section 8 of the *Charter*, not section 7.

The "adversarial relationship" factor works in a similar manner. When the encrypted data was created, the suspect and police were not adversaries.[146] Further, when the data is seized, there is no adversarial relationship beyond that arising in any case in which police suspect wrongdoing and exercise search and seizure powers to obtain evidence of it. An adversarial relationship producing self-incriminating information (i.e., the fact that suspect could decrypt and the inferences arising therefrom) develops only after police compel the suspect to decrypt.

The risk of unreliable confessions, the third factor in the *Fitzpatrick* analysis, is not material to any aspect of compelled decryption. This factor has two iterations. First, compulsion by state actors may lead to false confessions that contribute to wrongful convictions.[147] This is not an issue for compelled decryption. Persons facing criminal punishment for failing to

---

[143] *White*, *supra* note 119 at para 43. See also *Fitzpatrick*, *supra* note 114 at para 43; *R v Hebert*, [1990] 2 SCR 151 at 175, [1990] 5 WWR 1 [*Hebert*]; *Jones*, *supra* note 125 at 250–51; *SAB*, *supra* note 120 at para 57.

[144] *Supra* note 114 at paras 34, 44–46; *White*, *supra* note 119 at paras 51–66.

[145] See *R v Jarvis*, 2002 SCC 73 at para 96, [2002] 3 SCR 757 [*Jarvis*] (to comply with ss 7 and 8 of the *Charter*, tax investigators seeking evidence of criminal liability must obtain warrants to seize financial records).

[146] See *Fitzpatrick*, *supra* note 114 at paras 34–36 (fishers are not in an adversarial relationship with the state when statutorily required to produce catch reports); *D'Amour*, *supra* note 121 at para 50 (benefits claimants and the state are not in an adversarial relationship when tax slips are created); *Oickle*, *supra* note 30 at para 36.

[147] See *Fitzpatrick*, *supra* note 114 at para 44; *White*, *supra* note 119 at para 62.

provide access to encrypted data have a strong incentive to provide the correct key, and providing the wrong one cannot contribute to a conviction for the offence under investigation.[148]

The second aspect of the reliability criteria relates to the state's need for accurate information for non-incriminating purposes. Without assurances of evidentiary immunity, compelled persons will often be reluctant to reveal self-incriminating information.[149] Immunity is therefore granted as a *quid pro quo* to induce evidence required for regulatory purposes or the prosecution of others.[150] Individuals provided with such immunity are assured that their statements cannot be used against them, even indirectly, and are therefore more likely to tell the truth.

This incentive is unnecessary in the context of compelled encryption: persons with the ability to decrypt will either comply with or refuse orders to do so. If they provide a "false" key, this will be immediately apparent. If a person refuses to do so despite the consequences, and authorities still wish to obtain plaintext for a non-incriminating purpose, such as the prosecution of another, they can offer immunity on an individual basis.[151]

The final factor to be considered is the abuse of state power. Statutory compulsion raises the spectre of two types of abuse. First, investigators clothed with inquisitorial powers may apply undue pressure to induce recalcitrant suspects to self-incriminate.[152] Even if this does not produce un-

---

[148] See *D'Amour*, *supra* note 121 ("[t]he potential use of the T4 slips in criminal proceedings against the appellant could have no effect on the accuracy of the information contained in those slips" at para 51). There is a possibility of wrongful conviction for failing to comply with a decryption order, however. Persons who wish to comply (for example because there is encrypted data contains no incriminating evidence) but are unable to do so (for example, because they forgot the password) could nonetheless be convicted. It would therefore be important to include a strong subjective *mens rea* element in the definition of the refusal offence, such as "knowingly" or "wilfully" refusing to comply with a lawful order. See e.g. *RIPA*, *supra* note 111, s 53(1). In combination with the onerous "beyond a reasonable doubt" standard of proof, this would greatly minimize the risk of wrongful convictions.

[149] See Penney, "Self-Incrimination, Part III", *supra* note 122 at 480–81; Steven Penney, "The Continuing Evolution of the s 7 Self-Incrimination Principle: *R v White*" (1999) 24 CR (5th) 247 (WL Can).

[150] See generally *Nedelcu*, *supra* note 127 (describing evidentiary immunity for compulsion as a *quid pro quo* in the context of s 13 of *Charter*).

[151] See Penney, "Self-Incrimination, Part III", *supra* note 122 at 484.

[152] See *Fitzpatrick*, *supra* note 114 at paras 42–46, 52; *White*, *supra* note 119 at paras 58, 64.

reliable confessions, some means of inducing cooperation may simply be inhumane.[153]

Once again, this concern does not arise with compelled decryption. The law would not require suspects to provide any information other than the key or plaintext. Unlike the duty to provide accident reports at issue in *White*, there is little danger that the presence of police could induce suspects to "provide a more extensive statement to police than legally required" under the legislation.[154] Suspects would either provide the correct key or not. If not, they would face potential punishment after being afforded the usual due process protections granted to persons charged with offences. While it is always possible that police may overreach in questioning contumacious suspects, a statutory obligation to decrypt is likely to diminish this risk, not enhance it. Under the current law, police anxious to decrypt data in the investigation of a serious crime may be tempted to use improper interrogation techniques to obtain the key. In a high proportion of cases, a statutory obligation to decrypt would obviate the need for such measures.

The second type of abuse involves the use of statutory compulsion to enable inquisitorial fishing expeditions.[155] This could occur, for example, if police used decryption orders to identify the one person out of many capable of unlocking an encrypted device. Ultimately, however, this raises concerns about privacy, not self-incrimination.[156] And as elaborated below, it

---

153 See Steven Penney, "What's Wrong with Self-Incrimination? The Wayward Path of Self-Incrimination Law in the Post-*Charter* Era: Part II: Self-Incrimination in Police Investigations" (2004) 48:3 Crim LQ 280 at 298. See also *R v Hodgson*, [1998] 2 SCR 449 at paras 18–24, 163 DLR (4th) 577; *Hebert*, *supra* note 143 at 171–74; *Singh*, *supra* note 31 at paras 30–31.

154 *Supra* note 118 at para 64. See also *Jarvis*, *supra* note 145 (describing a statutory provision requiring taxpayers to answer "all proper questions" at para 53); Penney, Rondinelli & Stribopoulos, *supra* note 28 ("[i]nvestigators clothed with broad inquisitorial powers are less likely to be satisfied by non-confessional responses than those entitled only to limited information" at 374–75).

155 See Ratushny, *supra* note 31 at 349; *S (RJ)*, *supra* note 120 at para 142; Penney, "Self-Incrimination, Part III", *supra* note 122 at 486–87.

156 See *SAB*, *supra* note 120 (applying the *Fitzpatrick* "abuse of power" factor to compelled taking of bodily samples for DNA analysis and concluding that "prior judicial authorization, circumscribed by strict requirements of reasonable and probable grounds and stringent limits on the potential use of the collected DNA evidence, ensures that the power to obtain bodily samples is not abused" at para 59).

is easy to design a compelled decryption regime that would all but eliminate this risk.[157]

The four factors from *Fitzpatrick* demonstrate, then, that compelled decryption raises only minimal concerns about self-incrimination. Forcing people to acknowledge possession of a decryption key is undoubtedly self-incriminatory: it requires them to say or do something that could assist the state in proving its case.[158] Jurists holding deontologically-oriented conceptions of self-incrimination, who typically view almost any form of compulsion to assist the state as inherently harmful,[159] would likely see this as sufficient to trigger section 7 protection. But those with more instrumentalist approaches might ask: "what is the real harm in compelling a password?"[160] In the absence of concerns for reliability or inhumane methods, why shouldn't the state be able to use compelled evidence of key possession to prove its case?[161]

We do not take sides on this debate in this article, however. Instead, we advance a proposal that we hope may be broadly acceptable. Assuming that forcing suspects to admit key possession violates the self-incrimination principle, courts should grant use and derivative use immunity to this fact. Police would be permitted, however, to compel decryption and plaintext information would be admissible.[162] The state would accordingly have access to the evidence it would have lawfully been entitled

---

[157] As discussed in Part II.B(3), *infra*, police would be required to establish a connection between the individual and the encrypted information *before* any order compelling decryption.

[158] See generally *R v P (MB)*, [1994] 1 SCR 555 at 577–79, 113 DLR (4th) 461.

[159] See e.g. Robert S Gerstein, "Privacy and Self-Incrimination" (1970) 80:2 Ethics 87 at 90; Robert S Gerstein, "The Demise of *Boyd*: Self-Incrimination and Private Papers in the Burger Court" (1979) 27:2 UCLA L Rev 343 at 343–44; Donald B Ayer, "The Fifth Amendment and the Inference of Guilt from Silence: *Griffin v California* After Fifteen Years" (1980) 78:6 Mich L Rev 841 at 843–44. For a summary of such approaches, see Steven Penney, "What's Wrong with Self-Incrimination? The Wayward Path of Self-Incrimination Law in the Post-*Charter* Era: Part I: Justifications for Rules Preventing Self-Incrimination" (2004) 48:2 Crim LQ 249 at 256–66 [Penney, "Self-Incrimination, Part I"].

[160] See e.g. David Dolinko, "Is There a Rationale for the Privilege Against Self-Incrimination?" (1986) 33:4 UCLA L Rev 1063 at 1103; Daniel J Seidmann & Alex Stein, "The Right to Silence Helps the Innocent: A Game-Theoretic Analysis of the Fifth Amendment Privilege" (2000) 114:2 Harv L Rev 430 at 451–55.

[161] See Penney, "Self-Incrimination, Part I", *supra* note 159 at 266.

[162] To be clear, "derivative" use immunity in these circumstances applies only to evidence derived from the *act* of decryption, i.e., the fact that the suspect had the capacity to decrypt the data and therefore was likely aware of its contents. It would not extend to the plaintext data itself, which pre-existed the compulsion and therefore cannot be said to derive from it.

to but for the encryption, and no more. Depending on one's views, denying the state evidence of key possession may not be necessary to protect against unjustified self-incrimination. But it would be unlikely to hamper many investigations or prosecutions. It is rarely difficult to prove that an accused had access to a device through other evidence.[163]

Interpreting section 7 to prohibit compelled decryption or provide evidentiary immunity to plaintext, on the other hand, would substantially constrain law enforcement without preventing any wrongful self-incrimination.[164] As the Supreme Court has held, even when the self-incrimination principle is violated, prohibiting compulsion outright, as opposed to granting evidentiary immunity, is justified only when the state's predominant purpose is to obtain self-incriminating evidence, rather than some other legitimate public purpose.[165] In the case of compelled decryption, that purpose is obvious: helping police render intelligible information that they are legally entitled to possess. Further, since the plaintext was created without state-imposed compulsion, immunizing it would do nothing to protect against self-incrimination. Nor would it help to advance any important societal interests like inducing helpful evidence for other purposes.[166] Instead, it would simply serve as a shield for wrongdoing.

---

163 See Kerr, "Dangerous Game", *supra* note 36.

164 In most circumstances, prohibiting compulsion and providing evidentiary immunity to plaintext amount to the same thing. Apart from instances where plaintext could be used against third parties, police would have no reason to compel it as it could not be used, directly or indirectly, against the suspect.

165 See *S (RJ)*, *supra* note 120 at paras 6–7; *R v Primeau*, [1995] 2 SCR 60 at para 20, 38 CR (4th) 189; *R v Jobin*, [1995] 2 SCR 78 at para 36, 169 AR 23; *Re Application under s 83.28 of the Criminal Code*, 2004 SCC 42 at para 71, [2004] 2 SCR 248. See also *Branch*, *supra* note 139 at paras 5–12; Paciocco & Stuesser, *supra* note 116 ("it will be a rare case where the accused can show ... that the predominant reason for his compulsion is to make him speak about his own criminality" at 330).

It is possible that compulsion may also be barred when it would prejudice the adjudicative fairness, i.e. reliability, of future proceedings. See *Branch*, *supra* note 139 at para 9; *Phillips v Nova Scotia (Commission of Inquiry into the Westray Mine Tragedy)*, [1995] 2 SCR 97 at para 86, 124 DLR (4th) 129, Cory J, concurring. See also Paciocco & Stuesser, *supra* note 116 at 328–30 (this concern is not relevant to compelled decryption).

166 See *Fitzpatrick*, *supra* note 114 (noting that prohibiting admission of compelled, self-incriminating fishing reports would "[leave] the state with no feasible means of enforcing specific quotas in certain fishing areas," and that it is "hard to see how this would be a desirable outcome" at para 48).

3. Privacy and Section 8 of the *Charter*

As we have seen, the act of giving law enforcement access to encrypted information has two components: the physical act of decryption and the communicative statement arising from that act. And as we have contended, it makes little sense to distinguish between the compulsion of plaintext information, biometric identifiers, passwords, and keys. In each case, the law would compel the suspect to transform specific data from ciphertext into plaintext. Consequently, each situation should be treated as a physical act of decryption. The question then becomes whether section 8 of the *Charter* provides any protection for this act beyond that provided by section 7 for the communicative statement.

As discussed in Part II.A(2), above, section 8 claimants must first show that state agents intruded onto their reasonable expectation of privacy. This can be a notoriously difficult inquiry involving a myriad of considerations,[167] including whether the information revealed invades the "biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state."[168] Such information typically consists of "intimate details" of a person's "lifestyle and personal choices,"[169] such as "intimate relations or political or religious opinions."[170]

In many cases the encrypted data at issue would have attracted a reasonable expectation of privacy. Police would consequently have been required to seize it in accordance with section 8 of the *Charter*. But whether police invaded a reasonable expectation of privacy in obtaining data, the question remains whether they do so when they compel a person to decrypt it.[171]

---

[167] See *Spencer* 2014, *supra* note 87 (factors relate to "(1) the subject matter of the alleged search; (2) the claimant's interest in the subject matter; (3) the claimant's subjective expectation of privacy in the subject matter; and (4) whether this subjective expectation of privacy was objectively reasonable, having regard to the totality of the circumstances" at para 18). See also Penney, "Cost-benefit Analysis", *supra* note 97 at 760–73.

[168] *R v Plant*, [1993] 3 SCR 281 at 293, 157 NR 321 [*Plant*]. See also *R v Tessling*, 2004 SCC 67 at para 63, [2004] 3 SCR 432; *Spencer* 2014, *supra* note 87 at para 27; *Cole*, *supra* note 82 at para 45; *Patrick*, *supra* note 82 at para 82, Abella J, concurring.

[169] *Plant*, *supra* note 168 at 293. See also *R v Kang-Brown*, 2008 SCC 18 at para 227, [2008] 1 SCR 456, Bastarache J dissenting.

[170] *Thomson Newspapers*, *supra* note 141 at 517. See also *Branch*, *supra* note 139 at para 62; *143471 Canada Inc v Quebec (AG); Tabah v Quebec (AG)*, [1994] 2 SCR 339 at 377, 90 CCC (3d) 1, Cory J, citing *Thomson Newspapers*, *supra* note 142 at 517–18; *Patrick*, *supra* note 82 at paras 30, 76; *R v Gomboc*, 2010 SCC 55 at paras 7, 121, [2010] 3 SCR 211 [*Gomboc*].

[171] Note that the reasonable expectation of privacy that would normally attach to inherently intimate information may be lost if the information is abandoned or knowingly ex-

In our view, they do. As discussed, an encryption key itself is non-communicative and thus does not itself reveal any reveal intimate, personal information. Nor does the decision to encrypt personal information necessarily create a reasonable expectation of privacy. We consequently argued in Part II.A(2) above that requiring encryption providers to facilitate law enforcement's lawful access to plaintext did not engage section 8 of the *Charter*.

But compelling encryption users to assist in decrypting data lawfully acquired by police invades privacy in a way that exceptional access does not. Exceptional access merely allows police who have already established their entitlement to specific data to obtain it in plaintext form. The police receive only information that would otherwise be available had the data never been encrypted. As discussed in Part II.B(2) above, however, compelling users to decrypt potentially provides police with new information: the fact that the user can decrypt. In addition to implicating self-incrimination, this information also raises privacy concerns under section 8.

In *R. v. Spencer* (2014), the Supreme Court concluded that a police request for an anonymous internet user's identity invaded a reasonable expectation of privacy because it allowed them to connect him to specific online activity.[172] Reasonable privacy expectations are similarly invaded when suspects are compelled to provide identifying information like fingerprints, bodily impressions, and bodily samples.[173] Unlike compelled decryption, these forms of compulsion implicate section 8 concerns for bodily integrity. Nonetheless, in determining their constitutionality under section 8, the Supreme Court has also taken note of the risk that the state may misuse intimate information gleaned from the identifying evidence.[174]

Consider what could happen if compelled decryption were *not* considered to invade a reasonable expectation of privacy. It would not be a "search or seizure" and could consequently never violate section 8 of the

---

posed to the public. See e.g. *Stillman*, *supra* note 127 at paras 55–62; *Patrick*, *supra* note 82 at paras 22–25. See also Penney, "Cost-benefit Analysis", *supra* note 97 at 770–73.

[172] *Supra* note 87 at paras 50–51, 66–67.

[173] See *R v Feeney*, [1997] 2 SCR 13 at para 60, 146 DLR (4th) 609 (taking of fingerprints); *Stillman*, *supra* note 127 at paras 52–65 (taking of a discarded tissue for DNA analysis and of dental impressions); *Dyment*, *supra* note 80 at 430–35 (taking of blood for alcohol analysis); *SAB*, *supra* note 119 at para 40 (taking of bodily samples for DNA analysis); *R v Borden*, [1994] 3 SCR 145 at 159–160, 119 DLR (4th) 74 (taking of bodily samples for DNA analysis).

[174] See *SAB*, *supra* note 120 at paras 40–43, 48–50.

Charter. Absent some other form of regulation, the state would be free to demand key disclosures from suspects without any evidence connecting them to the encrypted data.[175] Many innocent people could face intrusive decryption demands, demands that could generate reasonable fears of arrest, conviction, and imprisonment for failing to provide the "correct" key. In some cases, police might also exercise their discretion in discriminatory ways, perhaps by deploying conscious or unconscious stereotypes to disproportionately target members of racial, ethnic, or religious minorities.[176]

Recognizing that compelled decryption invades a reasonable expectation of privacy, on the other hand, would allow courts to regulate the practice through section 8's reasonableness requirement. Presumptively, this would require the compulsion to be preauthorized by a judge or justice, or other impartial arbiter capable of acting judicially, on the standard of reasonable and probable grounds.[177] In other words, police would have to obtain a warrant[178] based on solid, objective grounds to believe that the suspect has the capacity to access encrypted data that police are lawfully entitled to possess.[179] Obtaining a warrant would prevent the police from engaging in fishing expeditions and diminish the number of innocent people subject to such demands.[180]

---

175 See generally *Duarte*, *supra* note 23 at 44–45; *R v Wong*, [1990] 3 SCR 36 at 47, 60 CCC (3d) 460; *Gomboc*, *supra* note 170 at para 20, Deschamps J.

176 See Steven Penney, "Reasonable Expectations of Privacy and Novel Search Technologies: An Economic Approach" (2007) 97:2 J Crim L & Criminology 477 at 526–27 (noting that warrant requirements greatly minimize the risk of discriminatory profiling).

177 See *Hunter*, *supra* note 80 at 160. The same result could be achieved under s 9 of the *Charter*, which gives everyone the right not to be "arbitrarily detained or imprisoned." Because anyone refusing to a demand to decrypt would face the possibility of arrest and imprisonment, s 9 would be violated if police could arbitrarily demand key disclosures. Legislation imposing a loss of liberty without requiring a consideration of standards or criteria would violate this norm. See *R v Swain*, [1991] 1 SCR 933 at 1013, 63 CCC (3d) 481; *R v Lyons*, [1987] 2 SCR 309 at 348, 44 DLR (4th) 193.

178 Note that judicial authorization for compelled decryption is required in Australia but not the United Kingdom. See *Crimes Act* (Cth), *supra* note 111, s 3LA(1) (Australia); *RIPA*, *supra* note 111, s 49(2), Schedule 2 (UK). In our view, however, there is no reason to depart from the principle pronounced in *Hunter, supra* note 80 at 160–61, that warrants should be required for most searches and seizures when it is "feasible" to obtain one. As with most warranted search powers, courts have upheld warrantless searches in exigent circumstances, including the imminent loss of evidence. See *R v Grant*, [1993] 3 SCR 223 at 241–42, [1993] 8 WWR 257.

179 Similar standards are used in the United Kingdom and Australian legislation. See *Crimes Act*, *supra* note 111, s 3LA(2)(b) (Australia); *RIPA*, *supra* note 111, s 49(2)(a) (UK).

180 As with the United Kingdom legislation, the Parliament of Canada may wish to consider imposing additional protections to any compelled disclosure regime, such as proportionality and investigative necessity requirements. See *RIPA*, *supra* note 111,

So constrained, compelled decryption would be reasonable under section 8 of the *Charter*. Where police have strong evidence that a suspect has access to encrypted data, and have independently established their lawful authority to obtain it, there is no compelling privacy-related justification to forbid compelled decryption. If section 8 permits police to defeat encryption by other means, it should also permit them to do by compelling people to decrypt their data.[181]

Conclusion

The trust and security that encryption provides is critical to human flourishing in the digital age. But encryption also has the potential to provide an impenetrable shield for wrongdoing and alter the consensus balance of interests embodied in constitutional criminal procedure. Ideally, encryption should not prevent police from making sense of information that they are lawfully entitled to possess.

Yet, governments should be wary of imposing solutions that would diminish encryption's many social benefits. Compelling technology companies to install backdoors risks exposing individual, government, and commercial data to malicious actors. At least for the present time, exceptional access presents too great a risk to the security of digital networks and data to justify its benefits to law enforcement. It also faces daunting logistical and jurisdictional hurdles likely to thwart its effectiveness and generate substantial social costs. Ultimately, however, we think it is up to Parliament to decide whether to implement a comprehensive exceptional access regime. While we advise strongly against it, there is likely no constitutional impediment to doing so.

Though only a partial solution, compelled decryption promises to enhance law enforcement's ability to lawfully access digital data while avoid-

---

s 49(2)(b)–(d) (UK). Though such provisions could be imposed as constitutional requirements under s 8 of the *Charter*, courts have been reluctant to do so in most circumstances. See e.g. *R v Lucas*, 2014 ONCA 561 at paras 78–101, 121 OR (3d) 303, leave to appeal to SCC refused, 35974 (22 January 2015) (omission of usual investigative necessity requirement for wiretaps in criminal organization investigations does not violate s 8); *R v Largie*, 2010 ONCA 548, 101 OR (3d) 561, leave to appeal to SCC refused, 34160 (16 June 2011) (investigative necessity not required under s 8 for consent intercepts). But see *Lavallee, Rackel & Heintz v Canada (AG); White, Ottenheimer & Baker v Canada (AG); R v Fink*, 2002 SCC 61 at paras 34–39, [2002] 3 SCR 209 (investigative necessity required under s 8 for searches of material potentially protected by lawyer-client privilege); *Araujo*, *supra* note 22 at para 26 (suggesting in *obiter* that investigative necessity is required under s 8 for wiretaps).

181 See generally Kerr, "Encryption", *supra* note 82 (the Fourth Amendment does not impede the government's access to encrypted information and does not bar the government from decrypting said information).

ing the dangers of exceptional access. If Parliament does wish to act, it would be wise to consider it. While compelled decryption does implicate the *Charter*'s self-incrimination and privacy protections, it should not be difficult to construct a constitutionally-compliant regime. In brief, such a regime would:

(1) save for exigent circumstances, require judicial preauthorization for compulsion based on reasonable and probable grounds that the individual can decrypt data that police are lawfully entitled to possess; and

(2) exclude evidence that an accused was compelled to decrypt the information in question, while allowing the plaintext to be admitted.

These restrictions would greatly diminish the risk that police might use compelled decryption in arbitrary, discriminatory, or otherwise abusive ways. To some, it may still seem intuitively wrong for the state to force individuals to give up their passwords, keys, or biometric identifiers. As long as police have independently established their right to the encrypted data and shown that the person to be compelled has the ability to decrypt it, however, this is a small price to pay to help preserve law enforcement's capacity to detect and deter crime.