5-2023

The Impact of Encryption Technologies on Criminal Investigations in Canada: A Balanced Approach to the 'Going Dark' Problem in Light of Self-Incrimination and Privacy Considerations

Laura Ellyson
Dalhousie University Schulich School of Law

The Impact of Encryption Technologies on Criminal Investigations in Canada: A Balanced Approach to the "Going Dark" Problem in Light of Self-Incrimination and Privacy Considerations

by

Laura Ellyson

Submitted in partial fulfilment of the requirements
for the degree of Doctor of Philosophy

at

Dalhousie University
Halifax, Nova Scotia
December, 2022

Dalhousie University is located in Mi'kma'ki,
the ancestral and unceded territory of the Mi'kmaq.
We are all Treaty people.

TABLE OF CONTENTS

LIST OF FIGURES

ABSTRACT

Encryption, a method of concealing information from unwanted eyes, has recently become more prevalent in society, following revelations of massive surveillance conducted by governments and the increasing number of attacks on companies holding their customers' digitized information. Encryption mechanisms have become more sophisticated and widely used by citizens who wish to keep their personal information private and secure. Conversely, criminals have also been using strong encryption mechanisms to hide their wrongdoing, which has made it harder for law enforcement officials to access evidence. This "going dark" phenomenon has impacted both the seizure of "data at rest" (i.e., data that is saved on a device) and the access to "data in transit" (i.e., communication data that is still being transmitted over a network).

By examining the technological underpinning of encryption technology and its beneficial impacts on society, this thesis proposes an analytical framework that would allow law enforcement to compel suspects to decrypt their data or devices in specific situations and under strict conditions. This framework is crafted to reflect the unique Canadian experience with the self-incrimination and to harmonize this principle with the protection against unreasonable search and seizure, both found within the *Canadian Charter of Rights and Freedoms*. Inspiration is drawn from comparable legal systems found within Australia, the United States, and the United Kingdom, while transnational and international considerations are also examined due to the inherent borderless nature of the internet.

Essentially, this thesis submits that alternatives to compelled decryption by suspects should be favoured to address the "going dark" problem and that strong encryption should remain available to the public. It is submitted that Parliament should create a strict framework applicable to compelled decryption which would allow law enforcement access to "data at rest" in its decrypted form, when no other alternative exists. It is also submitted that resorting to "lawful hacking" as a method of circumventing encryption applied to "data in transit" should be examined and regulated by Parliament.

LIST OF ABBREVIATIONS USED

AES	Advanced Encryption Standard
ALRC	Australian Law Reform Commission
CACP	Canadian Association of Chiefs of Police
CALEA	*Communications Assistance for Law Enforcement Act* (US)
CBC	Canadian Broadcasting Corporation
DNA	Deoxyribonucleic Acid
ECHR	*European Convention on Human Rights*
E2EE	End-to-End Encryption
LAED Act	*Lawful Access to Encrypted Data Act* (US)
SCC	Supreme Court of Canada
FBI	Federal Bureau of Investigation
IGA	International Assistance Group (Justice Canada)
ISP	Internet Service Provider
IPA	*Investigatory Powers Act 2016* (UK)
IoT	Internet of Things
MDI	Mobile Device Identifier
MLA	Mutual Legal Assistance
NIST	American National Institute of Standards and Technology
NIT	Network Investigative Technique
OS	Operating System
PIPEDA	*Personal Information Protection and Electronic Documents Act*
RIPA	*Regulation of Investigatory Powers Act 2000* (UK)

RCMP	Royal Canadian Mounted Police
SGES	Solicitor General's Enforcement Standards
TAN	Technical Assistance Notice
TAR	Technical Assistance Request
TCN	Technical Capability Notice
TPDC	Third Party Data Custodian
TOLA	*Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Australia)
UN	United Nations
UK	United Kingdom
US	United States
VoIP	Voice Over Internet Protocol

ACKNOWLEDGEMENTS

Getting here has not been easy, nor is finding the right words to express my gratitude to the many individuals who have helped me along the sinuous path of doctoral studies. I owe a lot to the people I have met along the way, most of the time by pure chance. Life is well made like that sometimes.

I would like to start by extending my warmest and deepest thanks to my supervisor, Professor Robert J. Currie. Without your reassuring words and unwavering patience, I would not have been able to complete this thesis. Thank you for trusting me and giving me the time and space I needed to do things on my own terms. I deeply appreciate your constant guidance throughout the past years. Thank you for never prying about the reasons I asked for more time to finish a task, it meant more than you think.

Thank you to my committee members Professors Adelina Iftene and Steve Coughlan. To Steve, thank you for your constructive criticism and for sharing your expertise on the subject of criminal procedure with me. Adelina, thank you for doing the same on the somewhat nebulous subject of self-incrimination. Without both your help I would not have been able to submit a thesis that is of sufficient quality. Thank you to Professor Steven Penney for agreeing to be the external examiner to this thesis.

J'aimerais ensuite remercier Professeure Lucie Guibault, qui m'a accueilli à bras ouverts dès que je suis arrivée à Schulich. Connexion instantanée probablement expliquée par une langue maternelle partagée, j'aimerais te remercier pour les conversations de corridors (et d'aéroport), les conseils bien dosés et ton enthousiasme envers mes projets.

I would also like to thank the entire Schulich community for welcoming me amongst you in 2018. While I haven't nearly been back as often as I would have like (*ahem*, global pandemic), I will always remember my time in Halifax fondly. There is just something about all of you that is so welcoming. Some would call it Maritime hospitality; I would call it Schulich hospitality.

On a more personal note, I want to thank my partner in [metaphorical] crime Jeffrey James Moscato. Thank you for being my person, my biggest cheerleader, my love. Thank you for reading my thesis for the sole reason that I wrote it. Thank you for being patient when I got anxious about my work (and about life in general…). I adore our life together and the unwavering support you have given me has been truly eye opening. I would not have been able to finish this project without you. Thank you. Thank you. Thank you.

En rafale: merci à ma famille choisie (Tatiana, Audrey, Marwa), ma famille imposée, mais désirée (maman, Jessica & cie, Thomas, grand-papa), mes amies de toujours (Caterine,

Isabelle, Valérie), aux connexions perdues, mais importantes (Jean Bernard), à Me Annie Emond, à Professeur Hugues Parent, aux belles de chez B&P (tout particulièrement Jessyca et Gabrielle) et à ma doctorante honorifique (Shiraz). Merci à mes étudiants de Polytechnique Montréal de me permettre de faire ce que j'aime.

Finally, I would like to dedicate this thesis to my dad. I miss you every day. Thank you for instilling your curiosity in me. I know you'd be proud.

CHAPTER 1 INTRODUCTION

In modern democracies, the law is often a middle ground between polarities, a compromise between opposed points of view on a specific subject. Society is indeed made of oppositions; oppositions between main political currents, right and left, atheism and religions, status quo and change… Society is in fact an ongoing compromise between individual needs and collective ones, of personal preferences and institutional decisions. Law in general and criminal law specifically are no exception. They both thrive on this antagonism, on the disagreement between divergent ideas and constructs. Nonetheless, law strives to reach a balance between these antagonisms, to create a viable system that can reconcile and harmonise divergent opinions.

In recent years, such opposition between conflicting perspectives has been readily apparent within the debate on encryption and access to data found in electronic devices by law enforcement.[1] While advocates of privacy will argue that encryption should be encouraged and police access to encrypted data should be kept to a minimum, proponents of security (equated here with the positive outcome of investigating, repressing, and punishing criminal behavior) will generally tolerate a more intrusive approach to compelled decryption. The rise of encryption in communication technology and electronic devices is undeniably a growing concern for law enforcement officials, who fear that relevant data will become inaccessible,[2]

[1] *R v Vu*, 2013 SCC 60, [2013] 3 SCR 657 at para 38 [*Vu*]. The expression "electronic devices" is used in this thesis to encompass any device that can process digital data and access the internet. Further, no distinction will be made between computers and cell phones, except where otherwise noted, following the Supreme Court of Canada's statements that they are equivalent due to modern cellular phones' capacities. See *R v Fearon*, 2014 SCC 77, [2014] 3 SCR 621 at para 54 [*Fearon*].

[2] There are indeed examples of cases where law enforcement officials were unable to access data due to encryption. The most famous being probably the San Bernardino shooting case in California. See Alina Selyukh, "A Year After San Bernardino and Apple-FBI, Where Are We on Encryption?", (3 December 2016), online:

thus complicating or even halting some investigations. This point of view, often referred to as a fear of "going dark,"[3] has prompted some deep interrogations regarding privacy and self-incrimination, in opposition to security and the state's obligation or duty to investigate and punish criminal activity.

In our day and age, our personal data is located in multiple places, ranging from cell phones to company servers located in countries all around the globe, and everywhere in between. We exchange messages and information using the internet every day without asking ourselves about the "path" that is used in order to do so. It is likely that many of us do not worry about the methods used by service providers to store our data or to channel our communications. However, law enforcement officials are definitely interested in the technical aspects of data

NPR.org <https://www.npr.org/sections/alltechconsidered/2016/12/03/504130977/a-year-after-san-bernardino-and-apple-fbi-where-are-we-on-encryption>; 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.

[3] James B Comey, *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?* (Brookings Institution, 2014) cited in *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to all Data and Communications*, by Harold Abelson et al (Cambridge: MIT Cybersecurity and Internet Policy Research Initiative, 2015). See also Joey L Blanch & Stephanie S Christensen, "Biometric Basics: Options to Gather Data from Digital Devices Locked by Biometric Key" (2018) 66 US Att'ys Bull 3 at 11; Christine W Chen, "The Graymail Problem Anew in a World Going Dark: Balancing the Interests of the Government and Defendants in Prosecutions Using Network Investigative Techniques (NITs)" (2017) 19:1 Colum Sci & Tech L Rev 185 at 193; Aloni Cohen & Sunoo Park, "Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries" (2018) 32:1 Harv JL & Tech 169 at 172; Lex Gill, "Law, Metaphor, and the Encrypted Machine" (2018) 55 Osgoode Hall LJ 440 at 172; *Shining a Light on the Encryption Debate: A Canadian Field Guide*, by Lex Gill, Tamir Israel & Christopher Parsons (Toronto: The Citizen Lab and the Canadian Internet Policy & Public Interest Clinic, 2018) at 21; Orin S Kerr, "Compelled Decryption and the Privilege Against Self-Incrimination" (2019) 97 Tex L Rev 767; Lydia Lichlyter, "Encryption, Guns, and Paper Shredders: Analogical Reasoning with Physically Dangerous Technologies" (2017) 31:1 Harv JL & Tech 259 at 269; Manpearl, *supra* note 2 at 67; David W Opderbeck, "Encryption Policy and Law Enforcement in the Cloud" (2017) 49:5 Conn L Rev 1657 at 1661; Steven Penney & Dylan Gibbs, "Law Enforcement Access to Encrypted Data: Legislative Responses and the Charter" (2017) 63 McGill LJ 201 at 226; Steven B Taylor, "Can You Keep a Secret: Some Wish to Ban Encryption Technology for Fears of Data Going Dark" (2016) 19 SMU Sci & Tech L Rev 215–250; Robert Diab, "The Road Not Taken: Missing Powers to Compel Decryption in Bill C-59, Ticking Bombs, and the Future of the Encryption Debate" (2019) 57:1 Alta L Rev 267 at 272.

sharing and storage, due to the fact that these methods can impact the accessibility of the data that is relevant to a criminal investigation.

Encryption can be defined as "the application of cryptographic algorithms (generally called a *cipher*) to transform data (*plaintext*) using a random character string (a *key*) into an incomprehensible form (*ciphertext*)."[4] It is used to protect information from being intruded upon by unauthorized third parties. Encryption has multiple positive applications, of course; for example, it allows us to safely make purchases online[5] or to hide our personal information from identity thieves. However, it can also be used to hide criminal activity and evidence.

The idea of concealing information from unwanted eyes by using some type of cipher is not new; some authors trace cryptography at least back to the Roman empire[6], ancient Greece[7], or the Spartan empire.[8] The dual nature of encryption has already been the subject of debates in the United States in 1990s, when the government attempted to mitigate the potential

[4] Gill, Israel & Parsons, *supra* note 3 at 1.
[5] *Ibid* at 16.
[6] Adam C Bonin, "Protecting Protections: First and Fifth Amendment Challenges to Cryptography Regulation" (1996) U Chi Legal F 495 at 497; David Colarusso, "Heads in the Cloud, a Coming Storm - The Interplay of Cloud Computing, Encryption, and the Fifth Amendment's Protection against Self-Incrimination" (2011) 17 BU J Sci & Tech L 69 at 78; John F Dooley, *History of Cryptography and Cryptanalysis: Codes, Ciphers, and Their Algorithms*, History of Computing (Cham, Switzerland: Springer, 2018) at 13; Gill, *supra* note 3 at 442; Jeffrey Kiok, "Missing the Metaphor: Compulsory Decryption and the Fifth Amendment" (2015) 24 BU Pub Int LJ 53 at 55; Nathan K McGregor, "Weak Protections of Strong Encryption: Passwords, Privacy, and the Fifth Amendment Privilege" (2010) 12 Vand J Ent & Tech L 581 at 597; David W Opderbeck, "The Skeleton in the Hard Drive: Encryption and the Fifth Amendment" (2018) 70 Fla L Rev 883 at 885; Nicholas Soares, "The Right to Remain Encrypted: The Self-Incrimination Doctrine in the Digital Age" (2012) 49 Am Crim L Rev 2001 at 2008; Michael Wachtel, "Give Me Your Password Because Congress Can Say So: An Analysis of Fifth Amendment Protection Afforded Individuals regarding Compelled Production of Encrypted Data and Possible Solutions to the Problem of Getting Data from Someone's Mind" (2013) 14 Pitt J Tech L & Pol'y 44 at 47; Timothy A Wiseman, "Encryption, Forced Decryption, and the Constitution" (2015) 11 ISJLP 525–575 at 528.
[7] Brendan M Palfreyman, "Lessons from the British and American Approaches to Compelled Decryption" (2009) 75 Brook L Rev 345 at 349.
[8] D Forest Wolfe, "The Government's Right to Read: Maintaining State Access to Digital Data in the Age of Impenetrable Encryption" (2000) 49 Emory LJ 711–744 at 714.

negative outcome of encryption by regulating the strength of available encryption mechanisms.[9] However, technological advancements as well as the social and political context of the last two decades have definitely favoured a rise in the use and increased accessibility of encryption, for virtually everyone, ranging from sophisticated criminals to law abiding citizens. Indeed, on one hand, we can easily presume that high-level criminals are more likely to use strong encryption software than average criminals.[10] Thus, law enforcement might have an added motivation to access the protected data because of the seriousness of the crimes that can be covered by strong encryption, such as crimes related to child pornography or elaborate fraud schemes.[11] On the other hand, there is also a rise in end-to-end encryption (E2EE),[12] enabled by default by various service providers, such as WhatsApp.[13] Consequently, data protected by encryption is now likely to feature in a wide variety of crimes, regardless of their severity.[14] This being said, it is probable that cyber criminals[15] have

[9] Gill, Israel & Parsons, *supra* note 3 at 23; Abelson et al, *supra* note 3 at 5; J Riley Atwood, "The Encryption Problem: Why the Courts and Technology Are Creating a Mess for Law Enforcement" (2015) 34 St Louis U Pub L Rev 407 at 432; Colarusso, *supra* note 6 at 96–97; Tom Foremski, "The Battle over Encryption Technologies" (1994) 8 Int'l YB L Computers & Tech 311–314 at 311; Gill, *supra* note 3 at 448; Opderbeck, *supra* note 3 at 1659; Manpearl, *supra* note 2 at 69.

[10] Susan W Brenner opined in 2012 that encryption is likely more common among cybercriminal than average "street" criminal. This might be true when it comes to more advanced encryption methods. However, encryption is now very mainstream and is used to some extent by everyone who uses digital devices. Susan W Brenner, "Encryption, Smart Phones, and the Fifth Amendment" (2012) 33 Whittier L Rev 525 at 529.

[11] This thesis does not focus on specific crimes, such as cybercrime or "traditional" crimes. Nowadays, it is fair to say that almost every investigation will uncover electronic evidence, whether that crime can be defined as a cybercrime or not.

[12] See Chapter 2 for explanations on the technical aspects of encryption, such as end-to-end encryption (E2EE).

[13] WhatsApp, "WhatsApp Security", online: *WhatsApp.com* <https://www.whatsapp.com/security/>.

[14] It is estimated that more than 50% of internet traffic is encrypted. See Sandvine, "The Global Internet Phenomena Report – October 2018", (2018), online: *Sandvine* <https://www.sandvine.com/hubfs/downloads/phenomena/2018-phenomena-report.pdf>. Further, an estimated 48% of users use a password to protect their devices. See Kaspersky, "Kaspersky Lab Finds Over Half of Consumers Don't Password-Protect their Mobile Devices", (2018), online: *Kaspersky* <https://usa.kaspersky.com/about/press-releases/2018_kaspersky-lab-finds-over-half-of-consumers-don-t-password-protect-their-mobile-devices>.

[15] I.e., criminals that use a computer to commit an illegal act. See *inter alia* Oona A Hathaway et al, "The Law of Cyber-Attack" (2012) 100:4 Calif L Rev at 833–834.

the means and the knowledge to use stronger encryption software than most criminals or regular citizens, in turn making it harder for law enforcement to decrypt their data without resorting to extraordinary measures.

Multiple entities can create encryption software. While the most evident are probably tech companies, such as Apple or Microsoft, which include encryption software directly onto their devices, it can also be internet service providers (ISPs) or other types of online service providers that store data for commercial purposes, which will collectively be called Third Party Data Custodians (TPDCs) in this thesis. For example, Amazon's cloud service platform protects customer data with encryption software when the data reaches its servers,[16] while Signal provides encryption for messages exchanged using its application.[17] This "server-side encryption", applied remotely by the TPDC, can also be used in conjunction with "client-side encryption", which is encryption that is deployed directly on a device.[18] Users can also add supplemental encryption software onto their devices, by either downloading it on the internet from an individual or a company, or, if they are very tech-savvy, by creating it themselves.

Encryption has various specific uses. First of all, encryption can be at the device level—which is also, as mentioned, called client-side encryption—such as when a computer or cell phone is "locked," and its contents are made unavailable without using a specific key or password to "unlock" the device. In this case, the encryption method protects "data at rest," which is data that is held in storage, in a static manner. The same principles can also be applied at a

[16] Amazon, "Protecting data using encryption", online: *Amazon* <https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html>.
[17] Andy Greenberg, "Hacker Lexicon: What Is the Signal Encryption Protocol?", (29 November 2020), online: *Wired* <https://www.wired.com/story/signal-encryption-protocol-hacker-lexicon/>.
[18] Gill, Israel & Parsons, *supra* note 3 at 4.

smaller scale, when encryption protects only certain data on a device, such as specific files or a particular partition on a hard drive.[19] Second, encryption can also be engaged in the communication process, therefore protecting "data in transit," i.e., data that is being exchanged on the internet and has yet to reach its destination. Third, encryption can also be used in conjunction with other technologies, such as cryptocurrencies,[20] cloud computing,[21] and other online services. While this is an oversimplification and nuances need to (and indeed will) be explained, this is the starting point of the problem that law enforcement is currently facing: in some cases, investigators will find themselves with evidence that is inaccessible because of various encryption measures.

When an investigation is halted by the encryption of a specific device, law enforcement officials have a few options. Authors Orin S. Kerr and Bruce Schneier identify six "encryption workarounds": "find the key, guess the key, compel the key, exploit a flaw in the encryption software, access plaintext while the device is in use, and locate another plaintext copy."[22] For Steven Penney and Dylan Gibbs, both from the University of Alberta, the various methods that law enforcement currently possesses to access encrypted data can be grouped into four categories: "(i) traditional investigative methods; (ii) third party assistance; (iii) exploiting vulnerabilities; and (iv) guessing the password."[23] Of course, it is also possible that every

[19] This thesis will generally use language related to locked devices, not specific encrypted data on an otherwise unencrypted device, but the same principles apply.
[20] Laurent Sacharoff, "Unlocking the Fifth Amendment: Passwords and Encrypted Devices" (2018) 87 Fordham L Rev 203 at 210; Nicholas J Ajello, "Fitting a Square Peg in a Round Hole: Bitcoin, Money Laundering, and the Fifth Amendment Privilege against Self-Incrimination" (2015) 80:2 Brook L Rev 435.
[21] Sacharoff, *supra* note 20 at 210; Colarusso, *supra* note 6.
[22] Orin S Kerr & Bruce Schneier, "Encryption Workarounds" (2018) 106 Geo LJ 989 at 991.
[23] Penney & Gibbs, *supra* note 3 at 206. For a similar analysis, see also Cohen & Park, *supra* note 3. In this case, the authors suggest four options when facing a locked device: "compel the target [...] (1) to reveal the password, (2) to use a fingerprint, (3) to produce the decrypted contents, or (4) to enter the password."

technique fails, and that the state is simply unable to access the encrypted data located on a device in its readable decrypted form.

Most interestingly for current purposes, the legality of some of these investigative techniques is questionable, to say the least. Indeed, the constitutionality of compelling individuals to unlock their device—whether by revealing their password to the authorities or by using a physical feature in the case of biometric authentication measures—is unclear and highly disputed at the moment. While this is the simplest and often the fastest way of accessing encrypted data, the *Canadian Charter of Rights and Freedoms*[24] might just prohibit law enforcement from using such measures. On the other hand, there is also a struggle to obtain relevant data from third parties, such as ISPs or TPDCs. Generally speaking, these businesses have an interest in protecting their customers' data and might be reluctant to help law enforcement without a legal obligation to do so.[25]

Specifically, this thesis will address the following question: during the course of a Canadian criminal investigation, how can law enforcement access relevant data that is protected by encryption software, such as passwords and biometric protection measures, put forth by either end-users or service providers, located on individual devices (such as cell phones and computers) or on remote servers, while respecting individual rights protected under the *Canadian Charter of Rights and Freedoms*? In turn, this will raise questions about the

[24] *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK).
[25] Maybe especially after the revelations made by Edward Snowden in 2013. See Amitai Etzioni, "End to End Encryption, the Wrong End" (2016) 67 SC L Rev 561 at 575.

protections against self-incrimination and unreasonable search and seizure, as well as the technical limitations linked to accessing encrypted data.

Multiple solutions to this conundrum have been proposed by authors in various jurisdictions, predominantly from the United States. Using a qualitative analysis of doctrinal, jurisprudential, and legislative sources, including some comparative considerations, this thesis will focus on what a Canadian approach on this subject might look like in a near future.[26] More specifically, this thesis will examine how it is possible to reconcile the competing values that are present in the debate about compelled decryption and other methods used to access data in its decrypted readable state.

This thesis will consider the Australian, English, and American approaches in a comparative perspective, in order to inform what a Canadian framework on compelled decryption and access to encrypted data by law enforcement in the course of a criminal investigation could look like. While the Australian landscape on individual rights and freedom is different from the Canadian experience, most notably because of the absence of a bill of rights enshrined in the Australian Constitution,[27] their forthright approach to the subject of compelled decrypted is specifically interesting because Australia decided to regulate compelled decryption by way of legislative action, similar to what has also been done in the United Kingdom. Conversely, the American tendency is to focus on constitutional interpretation by way of the Courts—rather than waiting for laws to be enacted—which has a definite counterpart in the Canadian

[26] It is important to note at this point that this thesis only addresses the criminal law aspect of encryption and does not focus on its consequences on national security.

[27] George Williams, "The Federal Parliament and the Protection of Human Rights" (1999), online: <https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp9899/99rp20>.

judicial tradition. Moreover, American jurisprudence on constitutional matters is often referred to by the SCC, in part because of the similarities between our *Charter* and their Constitution.[28] This—combined with the abundant American doctrinal material on encryption—makes American sources unavoidable in any comparative examination of compelled decryption and other methods of accessing decrypted data.

Most importantly the protection against unreasonable searches and seizures (section 8 of the *Charter*) and the right against self-incrimination (section 7 of the *Charter*) will be analyzed to see if together,[29] or separately, they can and should provide sufficient basis to bar law enforcement from compelling suspects and TPDCs to produce decrypted data. While it is clear that data found on personal devices can be protected by s. 8 of the *Charter*,[30] this thesis will address the remaining question of whether the compelled act of decryption can be conceived as a search or a seizure under s. 8 of the *Charter*, thus restricting how law enforcement can access such information.[31] It will also consider if the protection against self-incrimination, as a principle of fundamental justice under s. 7 of the *Charter* that serves as a foundation for

[28] Jerome Atrens, "A Comparison of Canadian and American Constitutional Law Relating to Search and Seizure" (1994) 1 Sw J L & Trade Am 29–48.

[29] There is indeed a doctrinal school of thought that postulates that the protection against self-incrimination and the right against unreasonable searches and seizures must be reunified or harmonized in order to address the problematic of the access to decrypted data. See *inter alia* Sacharoff, *supra* note 20 at 206. This trend will be considered throughout this thesis and specifically in Chapter 7.

[30] *Vu*, *supra* note 1; *R v Morelli*, 2010 SCC 8, [2010] 1 SCR 253 [*Morelli*]; *R v Cole*, 2012 SCC 53, [2012] 3 SCR 34 [*Cole*].

[31] Indeed, the finding that compelled decryption would constitute a search or seizure would not completely bar law enforcement from accessing said data. It would only mean that certain norms and procedures need to be followed by law enforcement, for example obtaining a warrant beforehand. See *inter alia R v Collins*, [1987] 1 SCR 265; *Hunter v Southam Inc*, [1984] 2 SCR 145 [*Hunter*].

numerous criminal procedure rules including the right to remain silent,[32] can play a part in protecting Canadians from compelled decryption.

To some degree, any legislative decision regarding access to encrypted or otherwise protected data will be influenced by political motives, rather than being purely based on legal considerations. Any potential framework in this area might well be malleable and could be interpreted in ways favouring both opposed viewpoints. That being said, there are still some legal concepts that will set a *de minimis* standard that will need to be respected in order to meet *Charter* requirements. Parliament could decide to go above these and decide to ban compelled decryption or the weakening of encryption altogether. Further, multiple factors (other than constitutional) will also need to be considered by the courts and policymakers when addressing this issue.[33] This thesis will explore these imperatives and will propose some measures that should be implemented in Canada in order to respect individual rights, without unnecessarily impeding the state's ability to investigate and prosecute crime.

The pragmatic framework that will be proposed in this thesis is based on five general principles. First, any approach to regulating law enforcement access to encrypted data needs to be **proactive**. Indeed, criminal law is generally more reactive than pre-emptive, in part because the legislator cannot foresee every issue before it comes to light and because of the principle that courts should avoid adjudicating on matters not specifically brought forward by parties. However, this reactiveness can create discrepancies in the long run, primarily because problems will be dealt with on a piecemeal basis by courts. For this reason, it will be argued

[32] Nicola Dalla Guarda, "Digital Encryption and the Freedom from Self-incrimination: Implications for the Future of Canadian Criminal Investigations and Prosecutions" (2014) 61 Crim LQ 119.
[33] Gill, Israel & Parsons, *supra* note 3 at 40.

that such a framework should be created rapidly by the legislator. Second, this framework needs to be **coherent**. This means that the framework needs to be holistic and avoid inconsistencies between similar concepts, such as making overly picky distinctions between the types of encryption mechanisms being used by a suspect. Third, the framework should strive to be **balanced** and reunite the diverging interests at play, mostly privacy and security. It must create a symmetrical relationship between these values and reconcile the fact that there is no absolute right to privacy, nor a right for the state to have access to the most efficient investigative technique. Finally, a framework needs to be **adaptable**, capable of evolving to follow technological advancements that are, as it is well-known, often difficult to foresee.

Specifically, the proposed framework will be underpinned by these five preliminary notions:

1) Due to the importance of the right to silence in Canada and the distinction between testimonial and non-testimonial self-incrimination, law enforcement should not be allowed to compel suspects to reveal a password by any other mean than by inputting it directly themselves in the device;
2) The nature of a device (whether a computer, a cell phone, a smartwatch, or any other object capable of accessing the internet) should not have an impact on the protection afforded to the data it contains;
3) Strong encryption for lawful purposes must still be possible and should not be made obsolete by legislation about decryption capacities and *backdoors*;[34]

[34] I.e., hidden pathways in software put forth by tech companies that make decryption possible and easier for law enforcement or, in other words, an encryption weak spot that can be used by law enforcement with the help of tech companies. See Chapter 2.

4) Regardless of the strong individual rights at play, there should not be a general prohibition of law enforcement of trying to access relevant data if it is encrypted;
5) Any framework on the subject of compelled decryption and of access to otherwise decrypted data should come from legislative action.

This thesis will proceed in three main parts. The first part, Chapters 1 through 6, will focus on technical and legal concepts and will set the basis for the ongoing analysis. The unavoidable tension in criminal law between privacy and security, grounded in the relevant criminal law and privacy doctrine, will be analyzed, as it is the backdrop for the analysis that follows thereafter, which focuses on the right against self-incrimination and the protection against unreasonable search and seizure. The second part, Chapters 7 and 8, will examine access by law enforcement to data at rest,[35] regardless of the device being used for storage. When applicable, distinctions will be made according to the method being used to access the encrypted data, whether that be a password or a biometric authentication measure. This part will examine the possibilities of forcing a suspect to decrypt their data and the question of

[35] This thesis uses the "data at rest" and "data in transit" (also sometimes called "data in motion") dichotomy to distinguish data that is stored (on a server or a device) and arrived at its final destination (at least temporarily), as opposed to communication data that is still moving between devices on a network (the internet or another type of network) and that law enforcement is trying to access during this transit. This is done to distinguish between the specific sub-issues that can be attributed to each type of data (see Alan Z Rozenshtein, "Wicked Crypto" [2019] 9:5 UC Irvine L Rev 1181 at 1194) and because encryption methods are not the same for both types of data (see Manpearl, *supra* note 2 at 68). However, it is important to note that the actual technological functioning of systems might not be as black and white. Indeed, it has been reported that even data located on servers might be moved around by TPDCs, thus blurring the lines between what is effectively in transit or at rest. See Robert J Currie, "Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the 'Next Frontier'?" (2016) CYIL 63 at 20–21; Orin Kerr, "The surprising implications of the Microsoft/Ireland warrant case", *Washington Post* [29 November 2016], online: <https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/11/29/the-surprising-implications-of-the-microsoftireland-warrant-case/>. Accordingly, some caveats might be noted along the way, when necessary. Furthermore, the Internet of Things [IoT] might also modify what can be considered to be "data at rest" or "data in transit," see Sona R Makker, "Overcoming Foggy Notions of Privacy: How Data Minimization Will Enable Privacy in the Internet of Things" [2017] 85:4 UMKC L Rev 895.

whether TPDCs can be compelled to assist the authorities, either by providing them with a copy of the decrypted data when available or by creating encryption software that leaves a backdoor accessible to law enforcement. The possibility of banning encryption or restricting it severely will also be examined, as well as the other investigative techniques that are available as a "workaround" to encryption, including the question of immunities and section 13 of the *Charter*.[36] The third part, consisting of Chapter 9, will look at the impact of encryption applied to data in transit and the challenges that face law enforcement when they are trying to intercept encrypted private communications during the course of investigations, following the legal requirement found within part VI of the *Criminal Code*.[37] The consequences of encryption on criminal procedure and evidence will be explained throughout this thesis, using the scant but relevant Canadian case law on the subject.

Ultimately, this thesis will advocate for a more proactive and unified approach to be implemented in Canada, ideally through legislative intervention that is informed by the Canadian doctrine on self-incrimination and the principles of search and seizure law. The suggested approach is two-fold, depending on the type of data law enforcement is seeking to obtain. First, for data at rest, it is suggested that a specific judicial authorization should be

[36] The specific problematic of compelled decryption of data at international borders will not be examined as part of this thesis. On this subject, see Steven G Stransky, "Border Searches and the Limits of Encryption in Protecting Privileged Information" (2018) 44:4 Litigation 15; Laura K Donohue, "Customs, Immigration, and Rights: Constitutional Limits on Electronic Border Searches" (2018) 128 Yale LJ F 961; Rebecca M Rowland, "Border Searches of Electronic Devices" (2019) 97:2 Wash U L Rev 545; Thomas Mann Miller, "Digital Border Searches after Riley v California" (2015) 90:4 Wash L Rev 1943; Nicolette Lotrionte, "The Sky's the Limit - The Border Search Doctrine and Cloud Computing" (2013) 78:2 Brook L Rev 663; Carolyn James, "Balancing Interests at the Border: Protecting Our Nation and Our Privacy in Border Searches of Electronic Devices" (2010) 27:1 Santa Clara Computer & High Tech LJ 219; John Duong, "The Intersection of the Fourth and Fifth Amendments in the Context of Encryption Personal Data at the Border" (2009) 2:1 Drexel L Rev 313; Ashley H Verdon, "International Travel with a Digital Briefcase: If Customs Officials Can Search a Laptop, Will the Right against Self-Incrimination Contravene This Authority" (2009) 37 Pepp L Rev 105.

[37] *Criminal Code*, RSC 1985, c C-46.

created to authorize law enforcement to compel a suspect to decrypt a device or data, in situations where no other method can reasonably allow access to the evidence in a decrypted thus readable state. Effectively, this means that compelled decryption should only be available when law enforcement officials have already tried and failed at decrypting a legally seized device, or when they have reasonable grounds to believe that alternative methods will indeed fail. Second, for data in transit, it is submitted that the use of "lawful hacking" techniques—i.e., the use of techniques that are usually employed by hackers to remotely access data, such as the use of computer viruses and other types of malware, by law enforcement—is most likely the best option that can allow law enforcement to access private communications in their decrypted form, in a manner that is the functional equivalent to an interception. Both these suggestions aim to strike the balance between the opposed interests at play, while recognizing the inherent benefits of encryption for society as a whole.

PART 1 – THE TECHNOLOGICAL AND LEGAL BACKDROP

CHAPTER 2 SOME TECHNICAL CONCEPTS

[E]ncryption holds the promise of absolute privacy.[38]

Encryption is the use of technology to conceal private information from unwanted eyes. Various encryption software exists that use different techniques and different methods of accessing the data, such as biometric authentication measures or traditional alphanumeric passcodes. What all these methods share is the goal of protecting data from intrusion. In turn, encryption has been said to prevent law enforcement officials from accessing data that is relevant for an investigation, even when they are lawfully allowed to seize it, either pursuant to a judicial authorization or a common law power.

While comprehension of how encryption works on a coding level is not required for this thesis, some general concepts still need to be explored to set the table for the ongoing analysis. This chapter will start with a brief overview of how encryption evolved to its current iteration before delving into the different types of encryption. Other related concepts, such as the rise of cloud computing and the use of encryption by default by third party data custodians (TPDCs) will also be touched upon, as well as the various ways of accessing the data, more specifically passcodes and biometric protection measures. Finally, the practise of using comparisons or metaphors as a way to explain technical concepts in law will be analyzed in

[38] Andrew J Ungberg, "Protecting Privacy through a Responsible Decryption Policy" (2009) 22 Harv JL & Tech 537 at 548.

order to explain why such mental shortcuts should be avoided when it comes to the regulation of encryption in a criminal law setting.

2.1 Encryption's Origins and History

Encryption is a subset of what is called cryptology, which is "the science of secret communications."[39] The use of cryptology can be traced back centuries, as its goal is simply to transform a message, called the plaintext, into an unintelligible new version, called the ciphertext.[40] Multiple people or groups may have an interest in hiding the contents of their correspondence: "governments, the military, and people in business […] [s]pies, lovers, and diplomats,"[41] but also anyone who might value their privacy. It is said that Julius Caesar used cryptology to write to his friends and political allies,[42] in the form of what is called a cipher.[43] The use of cryptology has also been linked to the Greeks, the Arabs, and monks in Europe, at times ranging from 200 BCE to 1292 AD.[44] Some even attribute cryptography techniques to the Egyptians as far back as 1900 BCE.[45]

---

[39] Dooley, *supra* note 6 at vii. The term "cryptography" originates from Greek and means "hidden writings." See Peter Swire & Kenesa Ahmad, "Encryption and Globalization" (2012) 13:2 Colum Sci & Tech L Rev 416 at 429.

[40] Dooley, *supra* note 6 at 5.

[41] *Ibid*.

[42] *Ibid* at 13.

[43] Unlike a code, which simply substitutes the plaintext words with codewords using a predetermine code in the form of numbers or letters (for example, if I say "apple", I mean "orange"), a cipher uses "small, fixed-length language elements that are divorced from the meaning of the word or phrase in the message." *Ibid* at 6–8, 13–14. For example, Julius Caesar famously used a substitution cipher where he substituted the letter he wanted to use with the fourth letter ahead (thus transforming the word "apple" into "DSSOH").

[44] *Ibid* at 14–18. See also Bonin, *supra* note 6 at 497; Colarusso, *supra* note 6 at 78; Gill, *supra* note 3 at 442; Kiok, *supra* note 6 at 55; McGregor, *supra* note 6 at 597; Opderbeck, *supra* note 6 at 885; Soares, *supra* note 6 at 2008; Wachtel, *supra* note 6 at 47; Wiseman, *supra* note 6 at 528; Palfreyman, *supra* note 7 at 349; Wolfe, *supra* note 8 at 714, all on the various uses of cryptology throughout history.

[45] Matthew J Weber, "Warning - Weak Password: The Courts' Indecipherable Approach to Encryption and the Fifth Amendment" (2016) 2016:2 U Ill JL Tech & Pol'y 455 at 458–459.

Cryptology was famously used during World War II by Germany with what is called the Enigma Machine.[46] Although the Enigma is maybe the most well-known of the encryption machines, it is far from being the only one that was employed throughout history. Cipher machines can be traced back as far as the 15th century, with machines such as Alberti's cipher disk.[47] However, it is undeniably the advent of the computer—and even more so of the internet—that allowed encryption to evolve into what we know today.

Modern computer encryption rests on algorithms[48] that are used to encrypt and decrypt the relevant data, and to generate encryption keys.[49] Multiple types of algorithms are available to developers but the current most widely used algorithm is the "Advanced Encryption Standard" (AES) that has been approved by the American National Institute of Standards and Technology (NIST) in 2000.[50] This encryption standard can use keys of 128, 192, and 256 bits to encrypt and decrypt data;[51] the longer the key, the harder it is to circumvent the algorithm using a brute force attack.[52] For example, it is said that "the number of possible

---

[46] Joseph Jarone, "An Act of Decryption Doctrine: Clarifying the Act of Production Doctrine's Application to Compelled Decryption" (2015) 10 FIU L Rev 767 at 768; Michael S Mahoney, "Compelling the Production of Passwords: Government's Ability to Compel the Production of Passwords Necessary to the Discovery of Encrypted Evidence in Criminal Proceedings, Merely a Choice of Words" (2003) 6 TM Cooley J Prac & Clinical L 83 at 88.

[47] Dooley, *supra* note 6 at 37, 137.

[48] The Merriam-Webster dictionary defines the word algorithm as "a procedure for solving a mathematical problem." It is also specified that, while applicable to any procedure, it is widely used nowadays to describe "the set of rules a machine (and especially a computer) follows to achieve a particular goal." Merriam-Webster, "Algorithm", online: <https://www.merriam-webster.com/dictionary/algorithm>.

[49] National Academies of Sciences, Engineering, and Medicine (US), ed, *Decrypting the encryption debate: a framework for decision makers*, Consensus study report (Washington, DC: National Academies Press, 2018) at 15.

[50] National Institute of Standards and Technology, "Advanced Encryption Standard (AES)", (26 November 2001), online: <https://www.nist.gov/publications/advanced-encryption-standard-aes>.

[51] *Ibid*.

[52] A brute force attack is defined as an attempt to try breaking the encryption by trying every possible key methodically. See Kerr & Schneier, *supra* note 22 at 994; Swire & Ahmad, *supra* note 39 at 430. Generally, the strength of an encryption system will depend, as mentioned, on the length of the key but also on the strength of

keys for a given string of ciphertext encrypted using the algorithm AES-128 is so large that it would take powerful supercomputers millions of billions of years and immense amounts of electricity to guess the correct key by exhaustive search."[53]

Prior to the 1990s, computer encryption was mostly used by intelligence agencies.[54] When encryption standards began to be used by other actors in the field of computer technology, some countries, including the United States, began to regulate the export of encryption software, by using legal instruments that were previously used in the context of weapons.[55] Various countries also "exercised strict control over the availability, development, and use of cryptography."[56] Eventually, these methods of limiting the use and strength of encryption became more difficult to justify because of the necessity of securing information travelling over the internet. However, this did not mean that countries stopped their efforts to regulate encryption. Indeed, in the 1990s, a number of countries tried to regulate the use of encryption for fear that encryption could hinder law enforcement.[57] The only difference is that the focus changed from regulating encryption through export control to regulating it through key

its algorithm. See Jill M Ryan, "Freedom to Speak Unintelligibly: The First Amendment Implications of Government-Controlled Encryption" (1996) 4:3 Wm & Mary Bill Rts J 1165 at 1173.

[53] Gill, Israel & Parsons, *supra* note 3 at 2.

[54] *Ibid* at 21.

[55] *Ibid* at 22; Bonin, *supra* note 6 at 500–501; National Academies of Sciences, Engineering, and Medicine (U.S.), *supra* note 49 at 7; Swire & Ahmad, *supra* note 39 at 438. See also, for example, "Export Controls on Cryptographic Goods", (23 December 1998), online: *Global Affairs Canada* <https://www.international.gc.ca/controls-controles/systems-systemes/excol-ceed/notices-avis/113.aspx?lang=eng>.

[56] Christopher Parsons, "Canada's New and Irresponsible Encryption Policy - How the Government of Canada's New Policy Threatens Charter Rights, Cybersecurity, Economic Growth, and Foreign Policy", (21 August 2019), online: *Citizen Lab* <https://citizenlab.ca/2019/08/canadas-new-and-irresponsible-encryption-policy-how-the-government-of-canadas-new-policy-threatens-charter-rights-cybersecurity-economic-growth-and-foreign-policy/>.

[57] Abelson et al, *supra* note 3 at 5.

escrow and decryption capacities.[58] This whole era, ranging from 1970 and culminating in the 1990s, is now dubbed as the "Crypto Wars."[59]

At that time, alongside the exponential growth of the internet, society saw its first debate between the public demand for stronger encryption and the governmental fear of losing surveillance and investigatory capacities. The government of the United States led the charge to restrict the use of encryption by proposing a key escrow scheme that rested on the "Clipper Chip", a computer chip that would have allowed for the strongest-known encryption algorithm to be implemented on devices, while also giving the government a copy of each device-specific encryption key, thus giving law enforcement the ability to decrypt communications and data.[60] On the other side, multiple groups were protesting for the recognition of privacy rights on the internet, including a group that called itself the *Cypherpunks*.[61]

Eventually, the Clipper Chip program was abandoned because flaws were discovered in its software and due to the strong opposition coming from libertarian groups and the industry.[62] The fear that the Clipper program would disadvantage American companies against

---

[58] As defined by Craig Jarvis, *Crypto wars: the fight for privacy in the digital age: a political history of digital encryption* (Boca Raton London New York: CRC Press / Taylor & Francis Group, 2021) at 161: "Key escrow is a system where encryption keys are stored by the government so they can access communications when they possess a warrant."

[59] Manpearl, *supra* note 2 at 68–69. Craig Jarvis in his book separates the Crypto Wars into three separate periods: the first crypto war that started in 1966 and ended in 1981; the second war that started in 1991 and finished in 2002; and the third war that started with the Snowden revelations in 2013 and is still ongoing. Jarvis, *supra* note 58 at 6. For the purposes of this thesis, exact dates are of little importance. Rather, what is relevant is the existence of this on-going debate or opposition between governments and privacy-rights activists. See also Swire & Ahmad, *supra* note 39 at 418, in which the authors also separate the crypto wars of the 1990s in three main stages according to the method favored by the government to regulate encryption.

[60] Gill, Israel & Parsons, *supra* note 3 at 23; Swire & Ahmad, *supra* note 39 at 434.

[61] Jarvis, *supra* note 58 at 5.

[62] Manpearl, *supra* note 2 at 69–70; Swire & Ahmad, *supra* note 39 at 435.

international competitors was also a concern,[63] in a climate where there was a global demand for strong encryption.[64] In 1999, the White House announced that all export restrictions on encryption software were lifted and it endorsed the idea that strong encryption is necessary in the digital age.[65] This halted the discussion about the regulation of encryption on devices for the time being, although decryption capacities for telecommunication carriers were effectively regulated through legislation in the United States and in Canada in the 1990s.[66]

Approximately a decade later, the debate about encryption re-emerged in its current iteration, in part because of the rise in encryption by default and the prevalence of end-to-end encryption (E2EE).[67] Encryption is not reserved to people with specific technical knowledge anymore and is largely installed on devices without the need for the consumer to do anything more than choosing a passcode or setting up a biometric authentication measure.[68] This new Crypto War is thus very different from its 1990s counterpart, *inter alia* because of the nature and the spread of the technologies used today.[69]

Multiple reasons explain why encryption has gained in popularity and is being used more widely by tech companies and consumers, including the backlash caused by Snowden

---

[63] Jarvis, *supra* note 58 at 179.
[64] Diab, *supra* note 3 at 271.
[65] Swire & Ahmad, *supra* note 39 at 440.
[66] Manpearl, *supra* note 2 at 70–71; *The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians*, by Christopher Parsons (Toronto: Telecom Transparency Project, 2015) at 34. For more information on the regulation of decryption capacities for telephone service providers, see Section 5.3.3 and Chapter 9.
[67] Manpearl, *supra* note 2 at 72. For definitions of these concepts, see *infra*.
[68] Encryption by default, quite contrarily to what was done in the past, rather requires positive action from the user to turn off encryption. *Ibid*.
[69] Justin Hurwitz, "EncryptionCongressMod (Apple + CALEA)" (2017) 30:2 Harv JL & Tech 355 at 371; Carlos Liguori, "Exploring Lawful Hacking as a Possible Answer to the 'Going Dark' Debate" (2020) 26:2 Mich Tech L Rev 317 at 323.

revelations in 2013.[70] When society was made aware of the sheer magnitude of the PRISM surveillance program and of Operation BULLRUN[71] implemented by the American government, there was a movement to claim stronger privacy protections for citizens.[72] In parallel, we are also seeing more and more private information leak from businesses after their servers are hacked, prompting these businesses to actualize and reinforce their security measures to reduce their liability.[73] Most notably, Apple and Google started encrypting communications with stronger means and more largely starting in 2010, with other smaller businesses following closely behind.[74]

In reaction to this trend towards stronger and more widely available encryption, law enforcement agencies grew more and more concerned about the possibility that data relevant to investigations will not be accessible in plaintext, even with the appropriate court order. Often cited as the most vocal figure of this "going dark" problem is then-Federal Bureau of Investigation (FBI) Director James Comey, who said:

> [u]nfortunately, the law hasn't kept pace with technology, and this disconnect has created a significant public safety problem… Those charged with protecting our

[70] Etzioni, *supra* note 25 at 575. For a summary of the revelations made by Edward Snowden, former NSA employee, see TC Sottek & Janus Kopfstein, "Everything you need to know about PRISM", (17 July 2013), online: *The Verge* <https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet>.

[71] Operation BULLRUN was conducted by the American National Security Agency (NSA) and aimed to break widely used internet encryption technologies, as well as influencing tech compagnies to insert vulnerabilities into their software. See Jarvis, *supra* note 58 at 324.

[72] Craig Jarvis argues that the impact of big events such as the Snowden revelations (or 9/11, for example) on the public's perception of privacy is not as clear as it may seem at first. *Ibid* at 9. In any case, it seems clear that the Snowden revelations are largely interpreted has having had some impact on the rise of encryption. See inter alia Liguori, *supra* note 70 at 323; Shannon Lear, "The Fight over Encryption: Reasons Why Congress Must Block the Government from Compelling Technology Companies to Create Backdoors into Their Devices" (2018) 66:2 Clev St L Rev 443; Taylor, *supra* note 3 at 217.

[73] National Academies of Sciences, Engineering, and Medicine (U.S.), *supra* note 49 at 40.

[74] Diab, *supra* note 3 at 272.

> people aren't always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority. We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so.[75]

In the United States, it appears that law enforcement agencies are indeed increasingly unable to access the data contained in devices, especially in phones. The National Academy of Sciences, Engineering, and Medicine reports that in 2016 the FBI was unable to gain access to the content of 885 devices out of 2 095 locked phones that were being examined by its forensic laboratory, and that in the same year the Manhattan District Attorney's was unable to circumvent the default encryption in 423 iPhones and iPads lawfully seized in a two-year period.[76]

Law enforcement agencies are also reporting being unable to access the content of communications that are legally intercepted with a wiretap. For example, the Administrative Office of the US Courts reported that "[p]olice were [technically] unable to decrypt 97 of the 102 encrypted wiretaps encountered in 2017."[77] The actual scale of the problem might, however, be underestimated, *inter alia* because law enforcement will not seek a wiretap warrant if they know that the communications are encrypted.[78]

More specifically in Canada, we are also seeing a renewed interest in the regulation of encryption. In 2016, a nationwide public safety consultation was carried out by the government of Canada. Among the issues addressed was the "diminished ability to investigate

---

[75] Comey, *supra* note 3, cited in Manpearl, *supra* note 2 at 74.
[76] National Academies of Sciences, Engineering, and Medicine (U.S.), *supra* note 49 at 41–42.
[77] Pam Dheri & Dave Cobey, "Lawful Access & Encryption in Canada: A Policy Framework Proposal" (2020) 68 Crim LQ 430 at 8.
[78] *Ibid*.

due to the use of encryption."[79] Recognizing that there is no provision in Canadian law that allows compulsory decryption,[80] the government was seeking the public's opinion about the circumstances, if any, where law enforcement should have the power to compel individuals or companies to assist law them with decryption.[81] The government also surveyed the opinion of Canadians regarding the possibility of reducing the effectiveness of encryption available to criminals, without limiting its beneficial uses for the public.[82]

Following the consultation, the government found that "a clear majority of participants oppose giving the government the capacity to intercept personal communications, even if a court authorizes the interception, and oppose any moves to weaken encryption technology."[83] Further, the consultations revealed that:

> A clear majority of civil liberties, legal, academic and industry organizations whose submissions addressed this issue believe strong encryption is vital to protecting privacy and maintaining freedom of expression. Many organizations opposed "back doors" for law enforcement because they would weaken network security and leave them vulnerable to attack, with industry organizations stressing that encryption technologies are essential to promote trust in the system. Law enforcement said that, while the Framework should seek to maintain security for law-abiding citizens, it should also give authorities the tools they need to access the communications of those who use secure communications technologies for criminal purposes.[84]

---

[79] Public Safety Canada*, Our Security, Our Rights National Security Green Paper, 2016.* (Ottawa, Canada: Public Safety Canada, 2016) at 57.
[80] *Ibid* at 61.
[81] *Ibid* at 64.
[82] *Ibid*.
[83] Public Safety Canada*, National Security Consultations - What We Learned Report* (Ottawa, Canada: Public Safety Canada, 2017) at 13.
[84] *Ibid* at 14.

In light of this, the government did not include powers to compel decryption in Bill C-59,[85] which aimed to overhaul national security legislation in Canada. Among other things, Bill C-59 modified the *Criminal Code* to allow for various measures designed to prevent the commission of acts of terrorism and to apprehend people suspect of committing such acts.[86]

In parallel, the Canadian Association of Chiefs of Police (CACP) adopted a resolution in 2016 calling for legislation that would allow for the compelled production of passwords or encryption keys, with a judicial authorization.[87] While the intrusiveness of the proposed measure is recognized, the CACP suggests that a framework balancing the opposed interests at play could be crafted.[88]

To support its position, the CACP alluded to situations where an investigation was indeed stopped or slowed because of encryption, including four Canadian cases. In the first case, police officers seized a hard drive during the execution of a warrant in a residence in Ontario, in relation to voyeurism charges. The hard drive was found to be encrypted and the technological crime unit could not break the encryption. Eventually, the hard drive was unlocked after officers found the necessary login information written down by the accused in

---

[85] Bill C-59, *An Act respecting national security matters*, 1st Sess, 42nd Parl, 2019 (assented to 21 June 2019), SC 2019, c 13; Diab, *supra* note 3. It is also important to note that similar decryption obligations were previously included in four bills that were never enacted. See Leah West & Craig Forcese, "Twisted into Knots: Canada's Challenges in Lawful Access to Encrypted Communications" (2019) Ott Fac L Work Paper No 2019-38 at 6.

[86] Tanya Dupuis et al, "Legislative Summary of Bill C-59: An Act respecting national security measures", (3 June 2019), online: *Parliament of Canada* <https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/LegislativeSummaries/421C59E>.

[87] Canadian Association of Chiefs of Police, *Resolutions Adopted at the 111th Annual Conference - Resolution #03-2016 - Reasonable Law to Address the Impact of Encrypted and Pass-Word Protected Electronic Devices* (Ottawa, Canada: Canadian Association of Chiefs of Police) at 22.

[88] *Ibid*.

a document.[89] In a Saskatchewan case, a child pornography investigation was stalled for two-and-a-half years before forensic technicians were able to decrypt the accused's computers, which led to a declaration of culpability.[90] However, in the two other cases cited by the CACP, Ontario law enforcement was unable to access the data, which even led to the devices being returned to the suspect in one of them.[91]

In the wake of the public consultations in 2016, three Canadian Broadcasting Corporation (CBC) News journalists also revealed a series of cases where the Royal Canadian Mounted Police (RCMP) was unable to access relevant data as part of its investigation. These cases pertain to accusations such as child abuse, financial fraud, and terrorism.[92] The CBC article was part of a series on police, power, and privacy, which also included testimony by Ontario's former privacy commissioner Ann Cavoukian and Micheal Vonn from the British Columbia Civil Liberties Association that refuted the RCMP's position based on the lack of evidence that communications are actually "going dark."[93]

According to Christopher Parsons, Canada had historically been in favour of strong encryption until the government changed course in 2019.[94] Following a meeting with his Five Eyes colleagues, the Minister of Public Safety signed a collective statement to the effect that "tech companies should include mechanisms in the design of their encrypted products and

---

[89] *Ibid*.
[90] *Ibid*.
[91] *Ibid* at 22–23.
[92] Dave Seglins, Robert Cribb & Chelsea Gomez, "Inside 10 cases where the RCMP hit a digital wall" (2016) CBC, online: <https://www.cbc.ca/news/investigates/police-power-privacy-rcmp-cases-1.3850783>.
[93] Dave Seglins, Robert Cribb & Chelsea Gomez, "RCMP want new powers to bypass digital roadblocks in terrorism, major crime cases" (2016) CBC, online: <https://www.cbc.ca/news/investigates/rcmp-digital-roadblocks-1.3850018>.
[94] Parsons, *supra* note 56.

services whereby governments, acting with appropriate legal authority, can obtain access to data, in a readable and usable format."[95] This statement appears to be in contradiction with a report issued by the Public Safety Committee in 2019 where it was stated that the government of Canada should "reject approaches to lawful access that would weaken cybersecurity" and where it was specifically made clear that strong encryption should be accessible for Canadians, even if that means law enforcement might face some additional challenges.[96]

To this day, no legislative framework on compelled decryption has been introduced in Canada.[97]

2.2 Encryption's Uses

The use of cryptology has always captured the collective psyche with cases such as the Zodiac Killer at the end of the 1960s,[98] movies such as *The Da Vinci Code*,[99] and the events that occurred in San Bernardino, California in 2015.[100] While publicized real-life events

[95] UK's Attorney General's Office, *Joint Meeting of Five Country Ministerial and quintet of Attorneys-General: communiqué, London 2019 (accessible version)* (United Kingdom: UK's Attorney General's Office, 2019) cited in Parsons, *supra* note 56.

[96] Standing Committee on Public Safety and National Security, *Cybersecurity in the Financial Sector as a National Security Issue* (Ottawa, Canada: Standing Committee on Public Safety and National Security, 2019) cited in Parsons, *supra* note 56.

[97] Although there are related powers. More on this *infra*. See also Diab, *supra* note 3 at 276.

[98] Michael Levenson, "51 Years Later, Coded Message Attributed to Zodiac Killer Has Been Solved, F.B.I. Says" *NY Times* (11 December 2020), online: <https://www.nytimes.com/2020/12/11/us/zodiac-killer-code-broken.html>.

[99] *The Da Vinci Code* (Sony Pictures, 2006).

[100] Ellen Nakashima, "Apple vows to resist FBI demand to crack iPhone linked to San Bernardino attacks", *Washington Post* (17 February 2016), online: <https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html?itid=lk_inline_manual_8>; Ellen Nakashima & Reed Albergotti, "The FBI wanted to unlock the San Bernardino shooter's iPhone. It turned to a little-known Australian firm.", *Washington Post* (14 April 2021), online: <https://www.washingtonpost.com/technology/2021/04/14/azimuth-san-bernardino-apple-iphone-fbi/>. Robert Diab gives a very succinct and clear timeline of the events that occurred in San Bernardino, California. To summarize, a terrorist shooting occurred in a governmental building and the terrorists were killed

surrounding encryption are usually criminal in nature, it must also be reminded that encryption has multiple positive applications.

Encryption is used to safely conduct business online, including protecting against fraud and IP theft,[101] to prevent unwanted intrusions into our devices by hackers and more largely to protect our privacy and our devices against any type of unauthorized access.[102] Encryption is linked to "confidentiality of information, […] data integrity [… and it] facilitates authenticity."[103] It also promotes economic growth and innovation,[104] "secures web traffic, maintains the confidentiality of files on a network, and protects electronic banking systems, for example."[105] As Steven Penney and Dylan Gibbs put it:

> 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. It also facilitates the expression of ideas and opinions and pursuit of fulfilling lifestyle choices essential to a free and liberal society.[106]

---

by the police. When the FBI recovered the iPhone of one of the shooters, they were not able to access its data. The FBI sought an order compelling Apple to assist with decrypting the phone, but Apple refused. Eventually, a third party helped the FBI to decrypt the phone, effectively ending the debate without a court decision on the subject of compelling tech-companies to help law enforcement with decryption. See Diab, *supra* note 3 at 274.

[101] Jamil N Jaffer & Daniel J Rosenthal, "Decrypting our Security: A Bipartisan Argument for a Rational Solution to the Encryption Challenge" (2016) 24:2 Cath U J of L & Tech 273 at 294.

[102] Brenner, *supra* note 10 at 530.

[103] Dheri & Cobey, *supra* note 77 at 6; National Academies of Sciences, Engineering, and Medicine (U.S.), *supra* note 49 at 30.

[104] Dheri & Cobey, *supra* note 77 at 7.

[105] Gill, *supra* note 3 at 444.

[106] Penney & Gibbs, *supra* note 3 at 203.

In short, without encryption the security of most of our day-to-day activities on our computer and on the internet would be compromised.[107] It is essential and at the centre of cybersecurity.[108]

Encryption also serves as a safeguard for multiple rights and freedoms. Apart from privacy rights,[109] encryption is also linked to freedom of speech,[110] freedom of association, and freedom of religion.[111] The United Nations (UN) Special Rapporteur and the High Commissioner for Human Rights recognize that encryption can provide anonymity for individuals and groups, which in turn can protect them against unlawful interference or attacks based on their opinions.[112] Amnesty International further recognizes that encryption is also linked to freedom of information and that it plays an important role in the work of human rights defenders.[113]

[107] See Swire & Ahmad, *supra* note 39 at 423–425 for a more details explanation about the importance of encryption for secure internet browsing.
[108] *Ibid* at 452–457.
[109] See Chapter 3 *infra*.
[110] Jarvis, *supra* note 58 at 8; Dheri & Cobey, *supra* note 77 at 6. Code itself is interpreted as being protected by freedom of speech. See Chapter 8 *infra*, as well as Etzioni, *supra* note 25 at 563; 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 McGill LJ 47.
[111] Dheri & Cobey, *supra* note 77 at 6; National Academies of Sciences, Engineering, and Medicine (U.S.), *supra* note 49 at 32.
[112] Dheri & Cobey, *supra* note 77 at 7 referring to the *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, by David Kaye, UN Doc A/HRC/29/32 (UNHRC, 29th Sess., 2015) at 5; *The Right to Privacy in the Digital Age*, A/HRC/39/29 (United Nations High Commissioner for Human Rights, 2018) at 6–7.
[113] Amnesty International*, Encryption: A Matter of Human Rights* (Amnesty International, 2016) at 14–15.

2.3 DIFFERENT TYPES OF ENCRYPTION

When it comes specifically to computer encryption, the transformation from plaintext to ciphertext uses a "random character string" called a key.[114] Without the correct key, the ciphertext holds no meaning to the human eye and can look like this:

```
hQIMAw3Jn/nLK/38ARAAsSXLDhCtzUYKMptNxZImJXwhhIRm3QxfuyHjJ93ASylE
e+6ABkuyFLJhiKryxp/JmS/alMPfF7hx2aTgovagaPzTwTV1jo6If2mhdCl6keed
1Iz7C0f6jHIqq9d8g0bWDyvELEipn5LNDTX3Xp2Csx5ojRB2wckrUtl1lXyj8G0H
4DQUYbINRmJVulJJC/acGvgOze66pHuRgSCxxHDscefjXenh/XejSYTo7aMi+Es7
DCcD49zH6ZLDQN6BlN9q2oFI8QIhQ2y1QJbat1dWi/4yYWlKZcLKRSm8eo/gNCdL
h9MncXBBSfgbvbu67CDZ9GO5geZOn3LzQOpJ8hrZq/6K/uMcUKeZjW3RCo0T754f
E5zYe1wUgtwS/lmQ2w5PQF/89bpshtDSYuL1fZgzrsE6DwophuCri5zwCGbEKlsI
g6REIETFbZ2aCL4N2pZVunCIEuoP0zgEB6+M9egdpyxMsMqEBVg3AH7Sa1AtEguP
T/MCxI0bZHCUhPupEKT8slbSrDNxTWMUXQt3XpL0bGCCrDMKLSoWYfDiNnRkFbWK
iiqw9hx4Q9CJg7xX7JRnVgwOeREiFnMYSbFlvPSxEOu6FdBYhdqSefKin4Wnkmdw
qrSl8fjIW/kZ2v72uz0buEKkY9ubBox76yjlRo9KUQMs3em03kc64959gTDiZ0qF
AgwDrosDPQ2BeYQBD/9H5VKFw0an5j5MX1JpOSBAqNGKWq2bcEFnwJfk0DDlhyHD
owHiG7gDowCS+5y/pf56v36HkzpJZATKqoRyKVxmQOxU9l3YnPc5fw8iFhxlrfcG
ywzkJh/BRDQ/uy5fhGc/PbSm6iLv/SkkWTK8PSUD+g1yZyK0W7WkMh9QYS2OE7lQ
qbwpNiy57reWkUWCoE4QmKqqpe7NXXM0eLT9l2D0hG2lthyvTvspkpxszl8+HMJv
M2LMcY2FmmZWAJSdxsQSq9NQdyvCJX2D8oa89WQyXmp7mPXL7BQfoQNPndmn6Obi
0EQojoeMRNh14XNhMjPjxW7m34rH2gtvdN3Dg8iFrtocoVJqXqU3N+9T2sNe/bS8
```

Figure 1 Ciphertext[115]

With the correct key, decryption (i.e., the act of converting the ciphertext into plaintext) is possible and makes the plaintext readily apparent, in the same manner you are currently able to read this thesis. Prior to decryption, it can be unclear if the plaintext is even meaningful at all.[116]

Encryption can exist at different levels, different moments, and with different methods. The following sections give an overview of these variations.

---

[114] Gill, Israel & Parsons, *supra* note 3 at 1.

[115] Andrew Hilts, "Ciphertext", (16 May 2018), online: *Citizen Lab* <https://citizenlab.ca/2018/05/shining-light-on-encryption-debate-canadian-field-guide/ciphertext/>.

[116] Cohen & Park, *supra* note 3 at 177.

2.3.1 Private Key and Public Key Encryption

Private key encryption is the most conventional method of encrypting data. Private key encryption is also called symmetric encryption because the key used to encrypt and decrypt the data is the same.[117] It is mostly used for data at rest (i.e., data that is held in storage on a device, either locally or on the cloud), due to the fact that it is based on one unique key. [118] If private key encryption was used to protect data in transit (i.e., data that is being transmitted on a network, usually the internet), the encryption key would need to be previously exchanged directly between individuals, for example in person or by courier, in order to provide a secure digital communication.[119] The other option would be to transmit the key "through nonsecure channels [which is] inherently flawed because communications could not begin without first risking the safety of the code as the deciphering mechanism itself could not be sent encrypted."[120]

Public key cryptography was initially theorized in 1976 by Whitfield Diffie and Martin Hellman, both from Stanford University.[121] It was suggested as the solution to the key exchange problem described here. Public key cryptography addresses the main flaw of private key encryption in relation to data in transit and removes the need to previously exchange encryption keys in secret. In public key cryptography, instead of keeping the single encryption

[117] Dheri & Cobey, *supra* note 77 at 5; National Academies of Sciences, Engineering, and Medicine (U.S.), *supra* note 49 at 16.
[118] Dheri & Cobey, *supra* note 77 at 5. For example, the AES uses symmetric encryption. Dooley, *supra* note 6 at 175.
[119] Jarvis, *supra* note 58 at 4–5. For example, the Enigma machine used by the Germans during WW2 used symmetric encryption, which means they needed to print codebooks to distribute the keys. See Swire & Ahmad, *supra* note 39 at 426.
[120] Bonin, *supra* note 6 at 497–498.
[121] Dooley, *supra* note 6 at 190.

key shared between users secret, two keys are used—a public and a private key—which allows for secure communications without the need to previously exchange the keys: the sender of a message will use the public key (known to everyone) to *encrypt*, while the receiver of the message will use the private key (known only to them) to *decrypt*.

As the name indicates, the public key is available to anyone who wants to correspond with the user and will be used to *encrypt* the data being send to the user. The public key can either be automatically generated by the software being used or provided by a designated authority.[122] On the other hand, the private key is known only to the user receiving the message and will be used to *decrypt* it. The two keys, while different, relate to one another in a way which makes it possible to decrypt the message encoded with the public key only when a user is in possession of the correct private key.[123] The corresponding public and private keys are created by specialized algorithms and thus do not need to be exchange in secrecy by users before engaging in a communication.[124]

Put differently, without the private key, the message encoded with the public key is unintelligible.[125] This means that if intercepted, the message will be unreadable to a third party, because they will lack the private key necessary to *decrypt* (even though they can access

---

[122] TechTarget, "Public Key", (June 2021), online: *TechTarget*, <https://www.techtarget.com/searchsecurity/definition/public-key#:~:text=The%20key%20can%20be%20generated,legitimacy%20of%20a%20digital%20signature.>.

[123] Jarvis, *supra* note 58 at 117. This is where Diffie and Hellman's contributions stopped. They did not provide with their publication an algorithm that was able to materialize public key encryption. This would have to wait until 1991 when Phil Zimmerman created Pretty Good Privacy (PGP), see *infra*.

[124] TechTarget, *supra* note 123.

[125] Bonin, *supra* note 6 at 498. While Adam C. Bonin states that there is no verified way to discover the private key from the public key, David Colarusso mentions that it is theoretically possible but difficult and impractical (Colarusso, *supra* note 6 at 80). In any case, public key encryption is widely recognized as being a very secure form of encryption for data in transit.

the public key used to *encrypt*). Public key encryption is also called asymmetric encryption because the public and the private key are different from one another: the first one is accessible to anyone (thus anyone can encrypt the message or data), while the private key is accessible to only one person (thus only that person can decrypt the message or data).[126]

Maximally simplified, private key encryption looks a little like this:

> imagine two political activists—Ameenah and Benjamin—who need to exchange email correspondence but are concerned about the risk of government surveillance. Using a public key encryption system like Pretty Good Privacy (PGP), Ameenah only needs to know Benjamin's public key (which he can make freely available on the Internet) in order to encrypt an email such that only Benjamin will be able to read it. Upon receipt of Ameenah's email, Benjamin can only decrypt the message using the private key file (which he kept secret) paired with his public one. Benjamin is then able to respond securely to Ameenah by using her public key to encrypt a message that only she can read.[127]

Or, in a more imaged way, public key encryption can be reduced to a simple diagram, which represents Diffie and Hellman's vision:

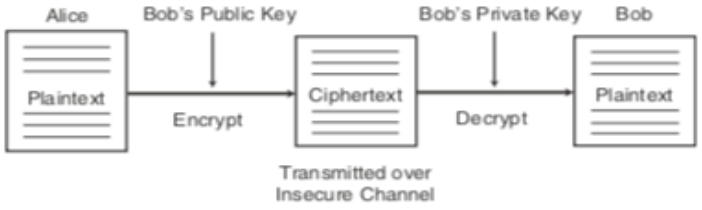

Figure 2 Basic model of public key cryptography[128]

[126] National Academies of Sciences, Engineering, and Medicine (U.S.), *supra* note 49 at 16.
[127] Gill, *supra* note 3 at 444.
[128] Dooley, *supra* note 6 at 189.

It is said that it is the advent of public key encryption that really launched the debate about the strength of encryption citizens should be allowed to use.[129] Public key encryption makes it easier to encrypt communications because the encryption key does not need to be disclosed on other channels before allowing for a secure communication to be established between individuals. In 1991, Phil Zimmerman, a member of the Cypherpunks, created "the first computationally viable public key cryptography software for personal computers,"[130] which is called Pretty Good Privacy (PGP). PGP is considered to have been a "radically democratizing tool," because of its easily accessible interface.[131] Zimmerman wrote the code of PGP with the idea in mind that people needed "to take their privacy into their own hands."[132] PGP also contributed to the lifting of encryption regulations in the United States.[133]

Unless they have a specific interest in understanding how encryption works and is applied to their devices and communications, users will usually not be aware if they are protected with public key or private key encryption. Indeed, the interface presented to users is typically simplified and does not necessarily reflect the type of encryption that underlies the application. For example, Transport Layer Security (TLS), which is used to secure communications over a network, uses public key cryptography automatically, without it being apparent for users.[134]

---

[129] Jarvis, *supra* note 58 at 5.
[130] *Ibid* at 6.
[131] Bonin, *supra* note 6 at 499.
[132] *Ibid*, citing Phil Zimmerman directly. The creation of PGP got Zimmerman into trouble with the American authorities, but the investigation and prosecution was eventually dropped. Jarvis, *supra* note 58 at 214–238. However, PGP has been called "dead" by some. See Amit Katwala, "We're calling it: PGP is dead", (17 May 2018), online: *Wired* <https://www.wired.co.uk/article/efail-pgp-vulnerability-outlook-thunderbird-smime>-its impact on the democratization of encryption is still important to this day.
[133] Swire & Ahmad, *supra* note 39 at 439.
[134] Gill, *supra* note 3 at 444.

Asymmetric (or public key encryption) is used to secure data in transit, including "web-browsing, emailing, and messaging."[135] This type of encryption is increasingly being applied by default directly by TPDCs.

2.3.2 Full Disk Encryption, File Level Encryption, and Device Level Encryption

Encryption can be employed to protect specific files, instead of the entire content of the device. "File level encryption" will allow anyone who has access to the device to see the location of the encrypted files, the names of the files, and possibly other related metadata,[136] but will protect the content of the file against unwanted access without the correct key.[137]

On a larger scale, it is also possible to encrypt an entire hard drive using encryption, which is called "full disk encryption." This type of encryption protects the entire device, including the operating system (OS),[138] which means it is a more complex encryption system.[139] Full disk encryption will also encrypt data, files, and software programs,[140] making the entire content of the device unavailable prior to decryption. This means that anyone who has access to the disk "would have no idea as to the number and size of the files on the disk, if any, their names,

[135] Dheri & Cobey, *supra* note 77 at 5.
[136] See definition of metadata *infra* at Section 2.3.2.
[137] Kaspersky, "Kaspersky Lab's File Level Encryption Technology", (2013), online: *Kaspersky* <https://media.kaspersky.com/en/business-security/Kaspersky-File-Level-Encryption-Technology.pdf>.
[138] What Is, "full-disk encryption (FDE)", (December 2014), online: *What Is* <https://whatis.techtarget.com/definition/full-disk-encryption-FDE>; John L Potapchuk, "A Second Bite at the Apple: Federal Courts' Authority to Compel Technical Assistance to Government Agents in Accessing Encrypted Smartphone Data under the All Writs Act" (2016) 57:4 Boston College L Rev 1403 at 1409.
[139] National Academies of Sciences, Engineering, and Medicine (U.S.), *supra* note 49 at 21.
[140] Antwanya Ford & LaTia Hutchinson, "Full disk encryption: do we need it?", (18 January 2018), online: *CSO Online* <https://www.csoonline.com/article/3247707/full-disk-encryption-do-we-need-it.html>.

or possible content."[141] In the case of file-level or disk-level encryption, the encryption software will use symmetric encryption.[142]

Protecting a device with a password is not always the equivalent of full disk encryption. Indeed, while mobile devices are now usually protected by default with full disk encryption,[143] computers are not necessarily automatically protected in the same way as soon as the user sets up a passcode. To put things simply, a password restricts the access to the content without changing its structure, while encryption will jumble the content to make it unintelligible.[144] Circumventing a simple passcode is very straightforward and can be as easy as physically removing the hard drive and plugging it in a different device.[145] By contrast, full disk encryption cannot be bypassed this effortlessly if an individual has gained physical access to the device. However, full disk encryption will not protect a user against unwanted access that comes from an attack on the networks they use,[146] for example if a hacker targets them with "malware."[147]

---

[141] Benjamin Folkinshteyn, "A Witness against Himself: A Case for Stronger Legal Protection of Encryption" (2013) 30 Santa Clara High Tech LJ 414 at 379; Opderbeck, *supra* note 6 at 889.

[142] National Academies of Sciences, Engineering, and Medicine (U.S.), *supra* note 49 at 20.

[143] For example, Apple has implemented full disk encryption by default with its iOS 9. See National Academies of Sciences, Engineering, and Medicine (U.S.), *supra* note 49.

[144] Randy Garland, "Encryption vs. Password Protection: A Matter of Acceptable Risk", (12 September 2014), online: *LinkedIn* <https://www.linkedin.com/pulse/20140912130912-9768674-encryption-vs-password-protection-a-matter-of-acceptable-risk/>.

[145] Micah Lee, "Encrypting your laptop like you mean it", (27 April 2015), online: *The Intercept* <https://theintercept.com/2015/04/27/encrypting-laptop-like-mean/>.

[146] For example, hackers could still gain access to the encrypted data using a virus or any other type of malware. See *ibid*.

[147] "Malware" is short for "malicious software," while hacking generally refers "to the manipulation and bypassing of systems to force those systems to do something unintended." While this term is generally used to represent something done unlawfully, it is worth stating that hacking can be done without committing a crime, for example by "white hat" hackers, who are simply hackers employed by companies to identify vulnerabilities in their systems. See Kaleigh E Aucoin, "The Spider's Parlor: Government Malware on the Dark Web" (2018) 69:5 Hastings LJ 1433 at 1441; Dan Rafter, "What is the difference between black, white and gray hat hackers?",

Encryption which is used to secure data at rest, whether it be at a disk or file level, is also called "endpoint encryption," to distinguish it from encryption that protects data-in-transit,[148] or client-side encryption.[149]

2.3.3 End-to-End Encryption

"End-to-end encryption" (E2EE) uses public key cryptography to protect data in transit.[150] It ensures that communications can only be read by the sender and the receiver of a message, which means that service providers or third parties intercepting the message cannot read the content of the communication,[151] "including law enforcement and intelligence agencies."[152]

E2EE used to be rare because of its complexity but has become increasingly available and accessible in the last decade.[153] A few examples of messaging services that use E2EE are iMessage, Signal, WhatsApp, and PGP,[154] as well as Facebook Messenger's secret conversations, Skype, and formerly Google Allo,[155] which is not in service anymore.

(25 February 2022), online: *Norton* <https://us.norton.com/internetsecurity-emerging-threats-black-white-and-gray-hat-hackers.html>.

[148] McAfee, "What is Endpoint Encryption?", online: *McAfee* <https://www.mcafee.com/enterprise/en-ca/security-awareness/endpoint/what-is-endpoint-encryption.html#types>.

[149] Gill, Israel & Parsons, *supra* note 3 at 4.

[150] Micah Hill-Smith, "Smartphone Encryption: A Legal Framework for Law Enforcement to Survive the 'Going Dark' Phenomenon" (2019) 25 Auckland U L Rev 173 at 176.

[151] Amnesty International, *supra* note 113 at 6–7; Parsons, *supra* note 56.

[152] Gill, *supra* note 3 at 445.

[153] Hill-Smith, *supra* note 150 at 176.

[154] Amnesty International, *supra* note 113 *at 6.*

[155] National Academies of Sciences, Engineering, and Medicine (U.S.), *supra* note 49 at 24.

2.3.4 Client-Server/Server-Client Encryption

A less-secure variant of encryption is "client-server/server-client encryption." This expression is used to describe the situation where a service provider retains the ability to decrypt the data that is travelling on its platform.[156] For example, the application Telegram uses client-server/server-client encryption, which means the communications are encrypted while in transit but are accessible to Telegram when stored on its own servers.[157]

2.3.5 Deniable Encryption and Hidden Volumes

"Deniable encryption" adds an extra layer to file level encryption by making the encrypted content completely hidden from view, except with the correct passcode. By applying deniable encryption, someone is capable of creating *hidden volumes*, which are partitions on a hard drive that are hidden from view, in such manner that it is possible to deny (thus the name) the existence of the hidden data.[158]

The passcode used to reveal the hidden volume will often be a second, different passcode from the one used for the rest of the device. This means that someone could pretend to decrypt their entire device by entering only a first passcode, while some parts of the hard drive would remain hidden and undiscoverable to third parties.[159]

---

[156] Gill, Israel & Parsons, *supra* note 3 at 6.
[157] *Ibid*.
[158] Alexei Czeskis et al, "Defeating Encrypted and Deniable File Systems: TrueCrypt v5.1a and the Case of the Tattling OS and Applications" (2008) 3rd Usenix Workshop on Hot Topics in Security, online: <https://www.schneier.com/academic/archives/2008/01/defeating_encrypted.html>.
[159] Cohen & Park, *supra* note 3 at 202–203; Sacharoff, *supra* note 20 at 222.

2.3.6 Perfect Forward Secrecy and Session Keys

"Perfect forward secrecy" is a method used to further secure asymmetric encryption. In regular asymmetric encryption, any past or future communication is compromised if a third party is able to gain access to the private key.[160] However, perfect forward secrecy addresses this concern by generating a new encryption key (called a session key) on a regular basis, which can be as often as with every new message sent or every new voice call.[161]

Wired reports that "practically every modern encrypted messaging app [now] uses perfect forward secrecy,"[162] which means that even if law enforcement was storing encrypted communications in the hopes of gaining access to the private key in the future, it is unlikely that they could ever decrypt the conversations because it would require law enforcement to gain access to every session key that was ever used on the device.[163]

Session keys can also be used without perfect forward secrecy in order to make asymmetric encryption faster and less resource consumptive, as "asymmetric encryption algorithms are generally computationally expensive compared to symmetric algorithms."[164] In that case, a session key is used to create a temporary symmetric session. This effectively means that if the communication was intercepted and the private key was discovered, the third party would be able to access the every message the session key encrypted. By opposition, perfect forward secrecy allows for the session key to be transmitted in a manner that protects the

---

[160] Gill, Israel & Parsons, *supra* note 3 at 8.
[161] Andy Greenberg, "Hacker Lexicon: What Is Perfect Forward Secrecy?", (28 November 2016), online: *Wired* <https://www.wired.com/2016/11/what-is-perfect-forward-secrecy/>.
[162] *Ibid*.
[163] National Academies of Sciences, Engineering, and Medicine (U.S.), *supra* note 49 at 24.
[164] Gill, Israel & Parsons, *supra* note 3 at 7.

communications fully (even with the private key, a third party could not access the communications without first gaining access to each and every previous session key).[165]

Perfect forward secrecy only protects data in transit. When arrived at its destination, endpoint encryption methods must be used in order to secure the data.[166]

2.3.7 Examples of Encryption Software Available Online

As mentioned, encryption is now often deployed by default on devices or communication applications. However, additional protection measures are also readily available on the internet for users to add onto their devices.[167]

TrueCrypt is a free encryption software easily accessible on the internet. It gives its users the possibility to encrypt volumes on their hard drive or to encrypt their entire computer system.[168] It is said that TrueCrypt's software is only accessible without the correct password via a brute force attack, which means that depending on the strength of the password employed, the encrypted content might be "uncrackable."[169] TrueCrypt, as well as the similar program VeraCrypt, also enable the use of hidden volumes.[170]

---

[165] Gill, Israel & Parsons, *supra* note 3 at 7–8.
[166] Opderbeck, *supra* note 3 at 1668.
[167] Christopher Parsons & Tamir Israel, "Canada's Quiet History of Weakening Communications Encryption", (11 August 2015), online: *Citizen Lab* <https://citizenlab.ca/2015/08/canadas-quiet-history-of-weakening-communications-encryption/>.
[168] Atwood, *supra* note 9 at 410–411.
[169] *Ibid* at 411. See also *R v Stemberger*, 2012 ONCJ 31 at para 51.
[170] Cohen & Park, *supra* note 3 at 201.

PC Mag reviewed 44 encryption software applications in 2021 and chose the nine best; in the lot two stood out: AxCrypt Premium and Folder Lock. [171] Both are available at low cost to encrypt files and folders on personal computers. AxCrypt can also be used to safely share encrypted files to other users using public key encryption.[172]

Encryption software reported in Canadian criminal law cases as being used by the accused or other people of interest are, *inter alia*, X-Shield,[173] PGP,[174] BestCrypt,[175] TrueCrypt,[176] Cryto,[177] as well as Virtual Private Networks (VPN) that allow for encrypted web browsing, in such manner that the user's IP address is hidden.[178]

2.3.8 Examples of Encryption Software Already on Devices or Applications by Default

First and foremost, an important disclaimer needs to be made at this point. Due to the nature of this thesis—which focuses on Canadian law, but also draws from comparative law in some commonwealth countries—the encryption techniques mentioned above and the software mentioned below should not be interpreted as being applied exactly in the same manner globally. Indeed, some countries still regulate encryption by restricting the strength of encryption keys that companies are allowed to use, by requiring service providers to modify

---

[171] Neil J Rubenking, "The Best Encryption Software for 2021", (19 October 2021), online: *PC Mag* <https://www.pcmag.com/picks/the-best-encryption-software>.

[172] See the "key sharing" features on AXCrypt's website. AxCrypt, "Features", online: *AxCrypt* <https://axcrypt.net/>.

[173] *R v Petrin*, 2016 ABQB 375 at para 78.

[174] *R v Tsekouras*, 2012 ONSC 5137 at para 4; *R v VL*, 2011 ONSC 218 at para 11; *R v Larsen*, 2011 SKPC 195 at para 9; *Williams c R*, 2018 NBCA 70; *R v Ferguson*, 2018 BCSC 594 at para 16.

[175] *R v Tang*, 2009 ONCJ 642 at para 51; *R v Beauchamp*, [2009] CanLII 64185 (ONSC) at para 172.

[176] *R v Pratchett*, 2016 SKPC 19 at para 66.

[177] *R v DO*, 2021 BCPC 171 at para 40.

[178] *R v Partanen*, 2021 BCPC 245 at para 6; *R v SE*, 2021 ONSC 4124 at paras 57, 61; *R c Faivre*, 2018 QCCQ 7467 at para 49. See National Academies of Sciences, Engineering, and Medicine (U.S.), *supra* note 49 at 22–23 for more information on VPNs.

their encryption techniques to allow for wiretapping and device-level searches, or by departing from encryption standards, all of which is presently not the case in Canada nor in the United States.[179] This means that an iPhone sold in India may not be protected by default with the same robustness as one acquired in Canada, for example.

FileVault is Apple's full-disk encryption system that is now available by default on all Mac computers running OS X Lion or later. In order to be functional, it needs to be activated by the user.[180] It encrypts the data on the startup disk, as well as all the information stored on the computer.[181] FileVault was reported being used by the accused in *R v Capancioni*.[182] Microsoft offers a similar encryption software called BitLocker.[183]

Apple also encrypts by default all iPhones that run iOS 8 or later, while Google does the same for any phone using its OS Android L or later.[184] This means that as soon as the user sets up a passcode or biometric authentication method, all the information stored on the device is encrypted.[185] Apple famously refuses to design their encryption software in a way that would allow for a third party, including themselves, to unlock a phone once locked.[186]

---

[179] Swire & Ahmad, *supra* note 39 at 418.
[180] Apple, "Use FileVault to encrypt the startup disk on your Mac", (18 November 2018), online: *Apple Support* <https://support.apple.com/en-ca/HT204837>.
[181]Apple, "How does FileVault encryption work on a Mac?", online: *Apple Support* <https://support.apple.com/en-ca/guide/mac-help/flvlt001/12.0/mac/12.0>.
[182] *R v Capancioni*, 2016 ONSC 4615 at para 22.
[183] Kerr & Schneier, *supra* note 22 at 993.
[184] Joe Miller, "Google and Apple to introduce default encryption", (19 September 2014), online: *BBC* <https://www.bbc.com/news/technology-29276955>.
[185] David Nield, "How to Get the Most Out of Your Smartphone's Encryption", (29 January 2020), online: *Wired* <https://www.wired.com/story/smartphone-encryption-apps/>.
[186] Lily Hay Newman, "The Apple-FBI Fight Is Different from the Last One", (16 January 2020), online: *Wired* <https://www.wired.com/story/apple-fbi-iphone-encryption-pensacola/>.

As mentioned previously, some communication services also use encryption by default to secure their customers' communications. Applications such as WhatsApp and Signal encrypt communications using E2EE by default, while other apps like Facebook Messenger, Telegram, and Skype require the user to turn on that functionality.[187]

2.4 Other Related Concepts

2.4.1 Data Stored on a Device and Data Stored on the Cloud

When computers first started being used, data was either saved locally on the device or on an external support, such as a floppy disk or a CD-ROM. However, the advent of the internet allowed for a radical delocalization of personal data to remote storage locations, often termed "cloud computing" or "cloud services." The former will be used here.

Cloud computing has multiple uses. It can be used as a platform for applications and software,[188] but also more simply for off-site storage of data. Because the data needs to transit between the user's computer and the cloud, encryption is necessary to protect the integrity and security of the data during that transfer, in the same way encryption is used when we access any webpage on the internet. Furthermore, encryption is also necessary on the cloud storage platform itself to protect the data at rest. This is even more true than for data that is saved locally because of the nature of cloud computing and the fact that cloud storage is usually provided by a third party (a "cloud service provider"). However, it must also be noted that "[d]epending on how the service is architected and the business model of the service

[187] Nield, *supra* note 185.

[188] For example, Dalhousie University uses Office 365 which allows users to use apps such as Microsoft Word, Excel, or PowerPoint directly on their web browser, instead of having to download the same app to their computer prior to utilization.

provider, the provider may or may not have access to the keys needed to decrypt the data."[189] Most notably, it is important to note that although Apple does automatically encrypt data stored or in transit to and from iCloud—its cloud computing platform—it does retain a copy of the encryption key and will communicate that information to law enforcement if presented with the appropriate court order.[190] By contrast, Google reportedly cannot access the data of its cloud computing customers.[191]

The use of cloud computing is particularly interesting when it comes to encrypted data because it can give law enforcement a different access point to data that they would be otherwise unable to decrypt. For example, it could be possible for law enforcement to access email through a court order directly from a TPDC if they are faced with a locked device that they are unable to crack.[192]

Encryption that is used to protect data at rest on the cloud is sometimes referred to as server-side encryption.[193]

2.4.2 Metadata and *Content Data*

The term metadata literally means data about data. With regards to communications, it is used to distinguish between the content of a communication and the non-content, such as time of the communication, the IP address used during the communication, or the phone number associated with that communication. In many cases, the metadata itself is not encrypted, even

[189] National Academies of Sciences, Engineering, and Medicine (U.S.), *supra* note 49 at 25.
[190] Nield, *supra* note 185.
[191] *Ibid*.
[192] National Academies of Sciences, Engineering, and Medicine (U.S.), *supra* note 49 at 41.
[193] Gill, Israel & Parsons, *supra* note 3 at 4.

if the content of the communication is.[194] This means that metadata will remain accessible to law enforcement even when they are unable to access the content of the communications because of E2EE.[195]

2.4.3 Vulnerabilities

"Vulnerabilities," or "exploits," are flaws that are found in the software of a program (whether the encryption software itself or another application found on a device) or directly on the device itself and that give access to the data in its decrypted form.[196] A vulnerability in a program will be called a zero-day vulnerability when it is discovered "prior to public awareness or disclosure to the vendor."[197] However, zero-day vulnerabilities are fairly rare because of the testing process software goes through before being released to the public.[198]

One common type of vulnerability is called a "backdoor." The term is used to identify vulnerabilities that are implemented deliberately by tech companies to allow access to the data found on a device or by communication service providers to give access to the data exchanged on their platform.[199] While the implementation of the backdoor is known by the company, it can still be qualified as a vulnerability because it effectively creates a weakness

[194] National Academies of Sciences, Engineering, and Medicine (U.S.), *supra* note 49 at 39.
[195] Amnesty International, *supra* note 113 at 18; Gill, Israel & Parsons, *supra* note 3 at 8.
[196] Penney & Gibbs, *supra* note 3 at 213.
[197] Liguori, *supra* note 70 at 333, citing Steven M Bellovin, Matt Blaze & Susan Landau, "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet" (2014) 12:1–2 Nw J Tech & Intell Prop 1 at 23. See also Hill-Smith, *supra* note 150 at 177.
[198] Liguori, *supra* note 70 at 333.
[199] Dheri & Cobey, *supra* note 77 at 4; Kerr & Schneier, *supra* note 22 at 1006.

in the software that can allow a third party, usually the government,[200] to access the data that is encrypted.[201]

2.5 PASSCODES

As mentioned, an encryption key is a "random character string"[202] of a specific length, (depending on the encryption standard used) that is created automatically by the encryption software. This means that the key itself is a long series of characters that is difficult, possibly impossible, to memorize.[203] For that reason, we normally substitute a passcode for the key.[204] The passcode usually does not unlock the device itself; rather "it unlocks the encryption key, which in turn unlocks everything on the disk."[205] This also means that encryption is only as strong as the passcode using to unlock the encryption key.

When it comes to full disk encryption, individuals should be aware of the fact that failing to remember the passcode used *in lieu* of the key might mean that they will never be able to recover the data saved on the device.[206]

Additional protections can also sometimes be added by a user. For example, if a feature is enabled by a user, the data contained on an iPhone can be automatically deleted if the user

---

[200] Opderbeck, *supra* note 3 at 1663.
[201] As explained in Section 2.7 *infra*, metaphors will generally be avoided in this thesis. However, the backdoor terminology (which is a metaphor in itself) will be used due to its frequent use and its clarity.
[202] Gill, Israel & Parsons, *supra* note 3 at 1.
[203] See for example Bill Buchanan, "So What Does a Modern Encryption Key Look Like?", (11 October 2018), online: *Medium* <https://medium.com/asecuritysite-when-bob-met-alice/so-what-does-a-modern-encryption-key-look-like-1c49efde9197>.
[204] Andreas Rivera, "A Small Business Guide to Computer Encryption", (29 January 2019), online: *Business News Daily* <https://www.businessnewsdaily.com/9391-computer-encryption-guide.html>.
[205] Lee, *supra* note 145. See also Kerr & Schneier, *supra* note 22 at 995; Sacharoff, *supra* note 20 at 221.
[206] Rivera, *supra* note 204; Ford & Hutchinson, *supra* note 140; Apple, "Encrypt Mac data with FileVault", online: *Apple Support* <https://support.apple.com/en-ca/guide/mac-help/mh11785/mac>.

fails to unlock the device after 10 passcode attempts. The user will then need to reset their device by connecting it to a computer.[207]

2.6 Biometric Authentication Methods

Biometric authentication methods are based on biometric information that can identify an individual using physiological characteristics that are deemed to be unique to an individual, including "fingerprint recognition, facial recognition, retina and iris recognition, and voice recognition."[208] Biometrics can be used to identify unknown people (one-to-many matching), for example when law enforcement uses fingerprinting to identity a suspect, or to confirm the identity of a specific person (one-to-one matching), which is the case when a user is unlocking their phone with a biometric feature.[209]

Biometric authentication methods started being used more widely as alternatives to more traditional passcodes in 2013 when Apple released its iPhone 5S which allowed users to scan their fingerprint and to use it to unlock their device.[210] This technology, called TouchID, allows for decryption of the device using the fingerprint of the user, but also uses encryption to locally store and protect the image of the finger used.[211] A few years later, Apple introduced FaceID with the release of its iPhone X. FaceID uses facial recognition instead of fingerprint

[207] National Academies of Sciences, Engineering, and Medicine (U.S.), *supra* note 49 at 22.
[208] Blanch & Christensen, *supra* note 3 at 3.
[209] David Feldman, "Considerations on the Emerging Implementation of Biometric Technology" (2003) 25:3 Hastings Comm & Ent LJ 653 at 655; Rudy Ng, "Catching up to Our Biometric Future: Fourth Amendment Privacy Rights and Biometric Identification Technology" (2005) 28:3 Hastings Comm & Ent LJ 425 at 428.
[210] Bilal Adra, "Facing the Facts on Biometric Phone Locks: Your Face and Thumb Are Not Secure" (2018) 2018:2 U Ill JL & Tech Pol'y 407 at 410.
[211] Kara Goldman, "Biometric Passwords and the Privilege against Self-Incrimination" (2015) 33 Cardozo Arts & Ent LJ 211 at 213.

recognition to unlock the device with a glance at the screen.[212] Since then, other tech companies have followed suit and have instituted biometric authentication methods on their devices.

When using a biometric authentication method, a user can still be required to enter their passcode instead of using the biometric feature. This happens mostly after too many failed attempts at using the biometric method, when turning on the device after it has been turned off, or by holding the power button as if the user was going to turn off their phone.[213] This can also be prompted if the user presses the power button of their device repeatedly.[214]

Generally, biometric authentication methods are deemed to be safer than passcodes from a technological point of view because of the uniqueness of the feature used, as opposed to the discoverability of using a passcode that can sometimes be easy to guess.[215] They are also more convenient for the user, mostly because of their instantaneity. However, biometric authentication methods are not perfect and are "subject to mistakes, fraud, and abuse through human and technological error, both intentional and inadvertent."[216] Further, once compromised, the biometric authentication method will never be safe to use again because users cannot change their biometric features.[217]

---

[212] Adra, *supra* note 210 at 410; Adam Herrera, "Biometric Passwords and the Fifth Amendment: How Technology Has Outgrown the Right to Be Free from Self-Incrimination" (2019) 66:3 UCLA L Rev 778 at 780.
[213] Richard G III Cole, "The Constitutional Insecurity of Secured Smartphones: Unlocking the Current Fourth and Fifth Amendment Safeguards Protecting Secured Smartphones from Law Enforcement Searches" (2018) 39:2 U of La Verne L Rev 173 at 181.
[214] Hill-Smith, *supra* note 150 at 173.
[215] Feldman, *supra* note 209 at 662; Herrera, *supra* note 212 at 784–786; Ariel N Redfern, "Face It - The Convenience of a Biometric Password May Mean Forfeiting Your Fifth Amendment Rights" (2021) 125:2 Penn St L Rev 597 at 603.
[216] Feldman, *supra* note 209 at 654–655.
[217] Kelsey Sherman, "Biometrics: The Future Is in Your Hands" (2017) 50:4 Loy LA L Rev 663 at 664.

Irrespective of the decision of the user to use a passcode or a biometric authentication method, the end result is the same. Indeed:

> [it] must also be recalled that regardless of whether a device is secured using an alphanumeric password, a passphrase, a fingerprint, a gesture, or even a facial scan as the mechanism from which the key is derived, encrypting the device involves precisely the same kind of mathematical transformation in all cases.[218]

The question then becomes whether these different methods of protecting data should have an impact on how we analyze encryption from a privacy or self-incrimination perspective.

2.7 Analogical Reasoning and its Impacts on the Law

Analogical reasoning is often used to explain technologically advanced concepts. Computer technology itself is full of comparisons with analog items: files, folders, chat rooms, the cloud, etc. As recognized by the Ontario Court of Justice:

> It is my information that computer programmers have worked hard to make information on computers appear as simple as possible through a number of real word metaphors or analogies. Data is presented as "documents" in "folders" and "filing cabinets" complete with icons that look like their namesakes. It is easy to confuse these visual aids with the reality of what is going on with the physical medium upon which the actual evidence is written.[219]

Encryption is not immune to this practise and has been compared to various physical objects, in addition to the various terms used to describe the different aspects of encryption themselves ("backdoor" or "encryption key", for example).

---

[218] Gill, *supra* note 3 at 470.
[219] *R v Bishop*, 2007 ONCJ 441 at para 28.

As mentioned previously, encryption has been categorized as ammunition by countries wishing to regulate it through export bans. The act of encryption has also been compared to translating a document, putting objects into a safe or a locked vault, shredding documents,[220] or even closing a telephone booth door.[221] These comparisons are sometimes made by software companies in order to explain their technology to the public, but they are also largely used by jurists in order to find the appropriate way of regulating this technology.

Metaphors are indeed often used in law, particularly but not exclusively the common law, because "[l]egal reasoning works explicitly by adapting old principles to novel facts: it operates through analogy, by way of precedent."[222] However, it has been argued that we should not compare encryption with "real-world" items, as metaphors do not reflect the true nature of encryption. As Jeffrey Kiok puts it:

> The dangers posed by the analogies and terms popularly used in computer software are not to be underestimated. Although computer users use language like 'folders' and 'containers,' unlike a real folder or container, the contents of an encrypted folder exist *only* in ciphertext, and not in plaintext. Thus, if one is presented with an encrypted hard drive, the readable plaintext *does not exist* on the hard drive; only ciphertext exists.[223]

---

[220] Folkinshteyn, *supra* note 141 at 399; Mahoney, *supra* note 46 at 89; Phillip R Reitinger, "Compelled Production of Plaintext and Keys" (1996) U Chi Legal F 171 at 173–174; McGregor, *supra* note 6 at 600–603; Efren Lemus, "When Fingerprints Are Key: Reinstating Privacy to the Privilege against Self-Incrimination in Light of Fingerprint Encryption in Smartphones" (2017) 70 SMU L Rev 533 at 542. See also Susan W Brenner, "The Fifth Amendment, Cell Phones and Search Incident: A Response to Password Protected" (2010) 96 Iowa Law Rev Bull 78 at 82, 86, who generally compares electronic devices with containers and the act of decryption with using a key.

[221] Karen G Lowell, "Civil Liberty or National Security: The Battle over iPhone Encryption" (2017) 33:2 Ga St U L Rev 485 at 502.

[222] Gill, *supra* note 3 at 455. See also Lichlyter, *supra* note 3 at 261.

[223] Kiok, *supra* note 6 at 59.

From another perspective, Lydia Lichlyter suggests that using analogies is perfectly acceptable, as long as we chose the proper analogy that adequately reflects the dangers and benefits of the two technologies we are comparing.[224] Aloni Cohen and Sunoo Park similarly agree that using analogies can sometimes be essential to understand a new technology, although they need to be chosen carefully in order to reflect the technical aspects of encryption.[225]

Choosing the right analogy when it comes to encryption is not an easy task. Comparing encryption to putting documents in a safe does not reflect how encryption effectively alters plaintext into ciphertext, as opposed to just locking it into a locked container, and the translation analogy does not reflect the robustness of the protection afforded by encryption.[226] The paper shredder analogy does come closer to adequately describe the act of encryption but does not reflect the speed or simplicity of the act of decryption.[227] The ammunition comparison does not reflect the positive values of encryption for society as it effectively puts encryption in the same category as weapons. The comparisons also completely fail to consider the technical aspects of encryption.

The problems with using analogies when analyzing the legal impacts of computer technology are known to Canadian law. The Supreme Court of Canada, in *R v Vu*, rejected a Crown analogy that computers are the same as physical "receptacles," holding that computer are not properly so analogized when it comes to search and seizure law.[228] Accordingly, this thesis

[224] Lichlyter, *supra* note 3.
[225] Cohen & Park, *supra* note 3 at 178–179.
[226] McGregor, *supra* note 6 at 584, 600–602.
[227] Kiok, *supra* note 6 at 77.
[228] *Vu*, *supra* note 1 at para 2.

generally adopts Kiok's suggestion that analogies should be avoided as they tend to be misleading and create mental shortcuts that do not adequately reflect the nature of this unique technology.

CHAPTER 3 THE INTRINSIC TENSION BETWEEN CRIME CONTROL AND PRIVACY IN CRIMINAL LAW

As suggested in the introduction, there is an intrinsic tension in criminal law between two opposed polarities: a societal struggle between the necessity of identifying offenders in order to control crime and the need to protect individual privacy and other *Charter*-related rights. This is evident from the jurisprudence on s. 8 of the *Charter* itself, which aims to "balance between the legitimate needs of law enforcement and the legitimate interest of 'everyone' in privacy."[229] Our adversarial criminal justice system is likely the ultimate embodiment of this dichotomy.

This opposition is also present when it comes to the regulation of encryption: some will favour an approach that allows law enforcement to access encrypted data rapidly and easily, while others will be proponents of privacy and will advocate for a right to encrypt private information and for procedures that make it harder for the state to access it.[230] In other words, the encryption debate also reveals the deeper debate of privacy versus security.[231]

This chapter will survey this tension as applied to the encryption debate. It will start with defining privacy and security, before exploring what has been said about the possibility (or

[229] *R v Kang-Brown*, 2008 SCC 18, [2008] 1 SCR 456 at para 24 [*Kang-Brown*].

[230] As suggested by P. Downes J. from the Ontario Court of Justice in *R v Shergill*, 2019 ONCJ 54 at paras 43–44, ultimately any decision about compelling a suspect to unlock a device is "a question of balancing the rights of the individual with the interests of society as a whole."

[231] Dan Terzian suggests that the core value of the US Fifth Amendment's protection against self-incrimination is to achieve a fair state-individual balance. The Fourth Amendment's protection against unreasonable searches and seizures would also seek to achieve this equilibrium. Dan Terzian, "The Fifth Amendment, Encryption, and the Forgotten State Interest" (2014) 61 UCLA L Rev Discourse 298–313 at 307. Ungberg also argues that the American privilege against self-incrimination is torn between the rights of the accused and the needs of law enforcement. See Ungberg, *supra* note 38. This section will examine if these conclusions can also be applied to the Canadian equivalent of these American rights.

impossibility) of striking a balance between these two values. Ultimately, the goal of this thesis is to determine how to strike the balance between these two values when it comes to the regulation of encryption and compelled decryption in Canadian criminal law. Thus, this chapter aims to survey these concepts in a broader manner, and to delve into how they inform the different values at play in the criminal justice system, such as the importance that our adversarial justice system places on the search for truth.

3.1 Defining Privacy

Defining privacy is notoriously difficult and proves challenging as this concept varies considerably between eras, cultures, and individuals. Privacy is indeed a broad concept that has evolved throughout history; from the simple act of withdrawing from the public eye to the birth of an individual right to privacy, and everything in between.[232] The humble ambition of this section is solely to survey what has been said about privacy in relation to criminal law and should not be seen as representing the broader scholarship on this subject. Further, the specific interpretation of privacy in the context of s. 8 of the *Charter* will be analyzed separately in Chapter 5.

Privacy was originally linked to specific places, such as our residences. For example, the Ancient Greeks considered the home to be separate from society but everything that happened outside the home was deemed to be in the public domain.[233] This idea is also reflected in *Semayne's Case*, in which it was stated that "every man's house is his castle."[234] Since then,

---

[232] Sacha Molitorisz, *Net privacy: how we can be free in an age of surveillance* (Montreal: McGill University Press, 2020) at 108–109.
[233] *Ibid* at 119.
[234] *Semayne's Case*, (1604), 5 Co Rep 91, 77 ER 194, cited *inter alia* in *R v Silveira*, [1995] 2 SCR 297 at para 41.

however, the right to privacy has evolved and is conceived as a personal right, thus not limited to a specific place.[235]

This modern individual right to privacy is often sourced to Samuel Warren and Louis D. Brandeis' 1890 article *The Right to Privacy*. In this text, the authors famously described privacy as a "right to be let alone."[236] This essay is acknowledged as being "*the* seminal force in the development of a 'right to privacy' in American law,"[237] but also more widely throughout the world. Indeed, Warren and Brandeis' article seems to have played a key role in the establishment of privacy as a legal principle worldwide.[238]

Multiple models have been proposed to define and delimit the contours of the right to privacy. Most germane here is the tendency to link privacy to the control individuals have over their information. Most notably, Alan Westin defined privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[239] The idea that privacy is, at least partly, defined by control has been used as a building block by many authors to craft their own model of privacy.[240] The

---

[235] See *inter alia Hunter*, *supra* note 31; *R v Edwards*, [1996] 1 SCR 128 at para 45 [*Edwards*].

[236] Samuel Warren & Louis Dembitz Brandeis, "The Right to Privacy" (1890) 4 Harv L Rev 193. In their article, the authors attribute the phrase to Judge Cooley but the sentence is often attributed to the authors' directly.

[237] Benjamin E Bratman, "Brandeis and Warren's The Right to Privacy and the Birth of the Right to Privacy" (2001) 69 Tenn L Rev 623 (italicized in the original).

[238] Molitorisz, *supra* note 232 at 118.

[239] Alan F Westin, *Privacy and Freedom* (New York: Atheneum, 1967) at 7.

[240] See for example Julie Inness, *Privacy, Intimacy, and Isolation* (New York: Oxford University Press, 1992) at 140, where the author defines privacy as "the state of possessing control over a realm of intimate decisions, which includes decisions about intimate access, intimate information, and intimate actions." See also Chris DL Hunt, "Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for the Development of Canada's Fledging Privacy Tort" (2011) 37:1 Queen's LJ 167 at 181–182; Lemus, *supra* note 220 at 559 quoting Charles Fried, Privacy, 77 Yale LJ 475, at 482; Adam D Moore, *Privacy Rights - Moral and Legal Foundations* (University Park, Pennsylvania: The Pennsylvania State University Press, 2010) at 25–27.

SCC also accepts control as being an important part of informational privacy on the internet, along with secrecy and anonymity.[241]

To reflect the multiple values at play when it comes to defining privacy, Daniel J. Solove proposed a taxonomy of privacy that uses family resemblances to identify the different elements that constitute privacy violations.[242] The taxonomy consists of four groups of harmful activities, each comprising more precise acts:

> (1) information collection (*surveillance, and interrogation*);
>
> (2) information processing, (*aggregation, identification, insecurity, secondary use, and exclusion*);
>
> (3) information dissemination (*breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation, and distortion*); and
>
> (4) invasion (*intrusion, and decisional interference*).[243]

This *ex-post* framework is interesting from a policy perspective because it allows us to conceive privacy is a more concrete way, as opposed to referring to broader or more abstract values that privacy should aim to protect. However, it does not provide a unified vision of what privacy is, nor does it attempt to do so.[244]

---

[241] *R v Spencer*, 2014 SCC 43, [2014] 2 SCR 212 at para 38 [*Spencer*].

[242] The family resemblance concept is used to describe privacy because it regroups characteristics that are related to one another, without sharing one unique defining element. See Daniel J Solove, "A Taxonomy of Privacy" (2006) 154:3 U Pa L Rev 477 at 486, referring to Ludwig Wittgenstein's work.

[243] Solove, *supra* note 242.

[244] Solove considers privacy to be "too complicated a concept to be boiled down to a single essence." *Ibid* at 485.

Privacy has also been described as being about access, rather than purely about control.[245] According to this point of view, privacy is about access to one's person, data, possession or space, not necessarily about control over these items.[246] In other words, "privacy is the condition of being protected from unwarranted access by others – either physical access, personal information, or attention."[247] Perceiving privacy in such manner entails that mass seizure of data by governments does not impact individual privacy rights, until the data is actually accessed by the state. *A contrario*, a control approach to privacy would deem the collection of information as problematic, even if it is never consulted.[248]

In any case, according to the SCC, access and control are not the sole factors to consider to determine if an individual possesses a reasonable expectation of privacy, nor they are "all or nothing concepts."[249] Thus, the Court adopts a holistic vision of privacy and defines it as being a right that is not solely expressed by the presence (of the absence) of one element; rather, the right to privacy must encompass different values and allow for a normative approach that is rooted in what society deems as private.[250]

Indeed, while the right to privacy relates directly to the individual and is thus an individualistic right by nature, it must also be comprehended as being informed by the interactions between

---

[245] See Chapter 5.
[246] Molitorisz, *supra* note 232 at 133.
[247] Molitorisz, *supra* note 232, citing Sissela Bok, *Secrets: On the ethics of concealment and revelation* (New York: Pantheon, 1982).
[248] Kevin MacNish, "Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World" (2018) 35:2 J App Philo 417.
[249] *R v Jones*, 2017 SCC 60 [2017] 2 SCR 696 at paras 40–45 [*Jones II*]; *R v TELUS Communications Co*, 2013 SCC 13, [2013] 2 SCR 3 [*TELUS*]; *Spencer*, *supra* note 241.
[250] *R v Reeves*, 2018 SCC 56, [2018] 3 SCR 531 at para 41 *in fine* [*Reeves*]. See also George Dolhai, "Why a New Approach to Privacy Rights and Section 8 of the Charter is Required in the Cyber Age and What It Could Look Like" (2020) 68 Crim LQ 29; *R v Tessling*, 2004 SCC 67, [2004] 3 SCR 432 [*Tessling*].

individuals and the society which they navigate.[251] Privacy rights cannot be conceived in a vacuum—where individuals are removed from their surroundings—but must reflect societal values and choices about what we can reasonably expect to be private: "privacy, properly understood, is relational."[252] Further, privacy can be seen as protecting social values—rather than only individual ones—such as setting boundaries for the state in the exercise of its power or promoting freedom of speech and association.[253]

This normative account of privacy takes into account moral or ethical considerations, as opposed to a descriptive or non-normative account of privacy that focuses rather on what is actually provided by a privacy measure.[254] As explained by Adam D. Moore:

> One way to clarify this distinction is to think of a case in which the term ''privacy'' is used in a non-normative way: ''When I was getting dressed at the doctor's office the other day, I was in a room with nice thick walls and a heavy door—I had some measure of privacy.'' Here it seems that the meaning is non-normative—the person is reporting that a condition obtained. Had someone breached this zone, the person might have said, ''You should not be here. Please respect my privacy!'' In this latter case, normative aspects would be stressed.[255]

---

[251] Molitorisz, *supra* note 232 at 120; Daniel J Solove, "I've Got Nothing to Hide and Other Misunderstandings of Privacy" (2007) 44:4 San Diego L Rev 745 at 760–764.

[252] Molitorisz, *supra* note 232 at 132. See also Solove, *supra* note 251 at 763 who states that "[p]rivacy, then, is not the trumpeting of the individual against society's interests, but the protection of the individual based on society's own norms and values."

[253] Arthur J Cockfield, "Protecting the Social Value of Privacy in the Context of State Investigations Using New Technologies" (2007) 40 UBC L Rev 41, referring to Priscilla Regan, Legislating Privacy: Technology, Social Values, and Public Policy (Chapel Hill: The University of North Carolina Press, 1995), at 221-230.

[254] Moore, *supra* note 240 at 14. For a descriptive account of privacy, see Daniel J. Solove's approach to the concept, explained in Michael Froomkin & Zak Colangelo, "Privacy as Safety" (2020) 95:1 Wash L Rev 141 at 148–149.

[255] Moore, *supra* note 240 at 14.

Conceiving privacy as reflecting societal values means that privacy is not static. Rather, privacy is an ever-evolving concept that must take into account the challenges brought forward by rapidly changing technologies, such as artificial intelligence,[256] Big Data analytics,[257] the Internet of Things (IoT),[258] and encryption. While there seems to be a collective disillusionment about how private our lives really are, due to surveillance enabled by communication technologies, accepting a normative vision of privacy means that privacy protections need to reflect what *should be*, rather than what *can be* or even *is*. In other words,

---

[256] *Repenser la protection des renseignements personnels à la lumière des défis soulevés par l'IA*, by Pierre-Luc Déziel, Karim Benyekhlef & Eve Gaumond (Laval: Observatoire international sur les impacts sociétaux de l'IA et du numérique, 2020); *Artificial Intelligence in the Context of Crime and Criminal Justice*, by Benoît Dupont et al (Korean Institute of Criminology, 2018); Andrea Scripa Els, "Artificial Intelligence as a Digital Privacy Protector" (2017) 31:1 Harv JL & Tech 217; Robert van den Hoven van Genderen, "Privacy and Data Protection in the Age of Pervasive Technologies in AI and Robotics" (2017) 3:3 European Data Protection L Rev (EDPL) 338.

[257] See *inter alia* Amy Conroy & Teresa Scassa, "Promoting Transparency While Protecting Privacy in Open Government in Canada" (2015) 53:1 Alta L Rev 175; Lisa M Austin, "Towards a Public Law of Privacy: Meeting the Big Data Challenge" (2015) 71:2 SCLR (2d) 541; Timothy J Kraft, "Big Data Analytics, Rising Crime, and Fourth Amendment Protections" (2017) 2017:1 U Ill J L Tech & Pol'y 249.

[258] The IoT can be defined as "the network of devices that contain the hardware, software, firmware, and actuators which allow the device to connect, interact, and freely exchange data and information." See NIST, "Internet of Things (IoT)", online: <https://csrc.nist.gov/glossary/term/internet_of_things_IoT>. Most authors will also agree that IoT devices contain sensors that allow the device to interact with the physical world without human control. On the interplay between the IoT and privacy, see Hillary Brill & Scott Jones, "Little Things and Big Challenges: Information Privacy and the Internet of Things" (2017) 66 Am U L Rev 1183; Larisa-Antonia Capisizu, "Legal Perspectives on the Internet of Things" (2018) Conf Int'l Dr 523; Laura DeNardis & Mark Raymond, "The Internet of Things as a Global Policy Frontier" (2017) 51 UCD L Rev 475; Stacy-Ann Elvy, "Commodifying Consumer Data in the Era of the Internet of Things" (2018) 59 BC L Rev 423; Steven I Friedland, "Drinking from the Fire Hose: How Massive Self-Surveillance from the Internet of Things is Changing the Face of Privacy" (2017) 119 W Va L Rev 891; Meg Leta Jones, "Privacy without Screens & the Internet of Other People's Things" (2015) 51 Idaho L Rev 639; Branden Ly, "Never Home Alone: Data Privacy Regulations for the Internet of Things" (2017) 2017 U Ill J L Tech & Pol'y 539; Lidiya Mischenko, "The Internet of Things: Where Privacy and Copyright Collide" (2016) 33 Santa Clara Computer & High Tech LJ 90; Sarit K Mizrahi, "Ontario's New Invasion of Privacy Torts: Do They Offer Monetary Redress for Violations Suffered via the Internet of Things?" (2018) 8:1 UWO J Leg Stud 3; Swaroop Poudel, "Internet of Things: Underlying Technologies, Interoperability, and Threats to Privacy and Security" (2016) 31 Berkeley Tech LJ 997; Steve Symanovitch, "The Future of IoT: 10 Predictions about the Internet of Things", (2019), online: *Norton Symantec* <https://us.norton.com/internetsecurity-iot-5-predictions-for-the-future-of-iot.html>; Adam D Thierer, "The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation" (2014) 21 Rich JL & Tech 1; Alexander H Tran, "The Internet of Things and Potential Remedies in Privacy Tort Law" (2017) 50 Colum JL & Soc Probs 263 on the impact of the internet of things on privacy.

"[m]erely because the state can locate, uncover or seize something, does not mean that it should be entitled to do so, at least in the absence of prior judicial authorization. Conversely, just because an individual can keep something secret does not mean that they should be permitted to do so."[259]

In the last few decades, communications have increasingly migrated to the digital sphere. Written communications have evolved from letters to text messages (SMS)[260] and emails, while oral conversations have shifted from landlines to Voice over IP (or VoIP) telephone services.[261] More recently, the global COVID-19 pandemic has prompted a dramatic shift to video conferencing, with platforms such as Zoom seeing their revenues explode overnight.[262] These profound changes in the way people interact with one another have impacted how criminal law approaches privacy, especially when it comes to the application of s. 8 of the *Charter*.[263] Suffice to say at this point that SCC decisions such as *Marakah* and *Mills II* reflect the normative shift that is occurring in society in regard to the way privacy is perceived.[264]

---

[259] Dolhai, *supra* note 250.

[260] *R v Marakah*, 2017 SCC 59, [2017] 2 SCR 608 at para 18 [*Marakah*]: "'Text messaging' refers to the electronic communications medium technically known as Short Message Service ('SMS'). SMS uses standardized communication protocols and mobile telephone service networks to transmit short text messages from one mobile phone to another..."

[261] "VoIP, in full Voice over Internet Protocol, also called IP telephony, communications technology for carrying voice telephone traffic over a data network such as the Internet." Encyclopedia Britannica, *VoIP communications* (2022), online: <https://www.britannica.com/technology/VoIP>.

[262] Rauf Arif, "In the Post COVID-19 World, Zoom is Here To Stay" (2021) Forbes, online: <https://www.forbes.com/sites/raufarif/2021/02/26/in-the-post-covid-19-world-zoom-is-here-to-stay/?sh=3a9c190055b5>.

[263] Privacy is also relevant to some offences themselves, such as voyeurism. See for example *R v Jarvis*, 2019 SCC 19 [2019] 1 SCR 488 [*Jarvis II*].

[264] *Marakah*, *supra* note 260; *R v Mills*, 2019 SCC 22, [2019] 2 SCR 320 [*Mills II*]. For more on this, see Chapter 5.

The rise of social media and of a culture of online sharing also challenges our relationship with privacy. However, the act of sharing information about oneself online does not mean privacy is becoming irrelevant or of lesser value. Users of social media still retain control on *what* they share, even if they do not have absolute control on *who* sees it.[265] Further, as Reem Zaia puts it, because a social media presence is very important for the development of young people, we should be wary of qualifying their expectation of privacy as being low or unreasonable regarding their online communications.[266] However, once something is effectively and voluntarily shared on social media, it will generally no longer be considered as private.[267]

Privacy is recognized as a fundamental human right, enshrined in international instruments such as the UN's *Universal Declaration of Human Rights*[268] and the *International Covenant on Civil and Political Rights*.[269] It is also accepted as a basic human right by most countries in Europe, through their respective constitutions,[270] and by multiple countries in different types of instruments or through jurisprudence.[271] Data privacy derives from this general

---

[265] On the subject of the apparent paradox of caring about privacy and sharing information about oneself, see Helen Fay Nissenbaum, *Privacy in context: technology, policy, and the integrity of social life* (Stanford, California: Stanford Law Books, 2010) at 187, cited in Froomkin & Colangelo, *supra* note 254. Here, Nissenbaum concludes that "there is no paradox in caring deeply about privacy and, at the same time, eagerly sharing information as long as the sharing and withholding conform with the principled conditions prescribed by governing contextual norms."

[266] Reem Zaia, "Constitutional and Quasi-Constitutional Privacy Protections: In Defence of a Heightened Expectation of Privacy for Young People Participating in the Digital World" (2020) 68 Crim LQ 362.

[267] *Marakah*, *supra* note 260 at para 55; *R v BH*, 2020 ONSC 4533 at para 17; *R v Adem*, 2021 ONCJ 210 at para 42; *R v Navia*, 2020 ABPC 20 at para 29.

[268] United Nations General Assembly, *Universal Declaration of Human Rights*, (10 December 1948).

[269] United Nations General Assembly, *International Covenant on Civil and Political Rights*, (16 December 1966).

[270] IE Vassilaki, "Crime Investigation versus Privacy Protection - An Analysis of Colliding Interests" (1994) 2:1 Eur J Crime Crim L & Crim Just 39 at 40.

[271] Alexandra Rengel, "Privacy as an International Human Right and the Right to Obscurity in Cyberspace" (2014) 2:2 GroJIL 33–54 at 41.

privacy right.[272] The concrete way privacy is protected will vary from one country to the next.[273] For example, privacy is not specifically mentioned in the *Canadian Charter of Rights and Freedoms* nor in the American Constitution, while it is expressively protected by the *Charter of Fundamental Rights of the European Union*.[274]

3.2 DEFINING SECURITY

In the context of encryption, security is mostly seen as having two different meanings. First, the security of society at large, encapsulated by the phrase "national security," is a preoccupation in this space. Privacy is often contrasted with national security using terrorism scenarios. Following this perspective, national security could be threatened by terrorists and cyberterrorists[275] who use encryption in such way that makes their communications or their data unreachable for law enforcement and national security agencies, preventing them from stopping the attack before it happens or allowing the terrorists to go unpunished.[276]

Second, security can also be interpreted as a positive outcome of the state's obligation to protect its citizens from harm, which includes the duty to investigate and prosecute crimes.[277]

---

[272] Erin Corken, "The Changing Expectation of Privacy: Keeping up with the Millennial Generation and Looking toward the Future" (2015) 42:2 N Ky L Rev 287 at 305.

[273] Vassilaki, *supra* note 270 at 40–42.

[274] European Parliament, *Charter of Fundamental Rights of the European Union*, C 326/391 (2012), s Title II, Art. 7.

[275] Generally, "cyberterrorism" can be defined as "the use of cyberspace in carrying out a terror attack". See Mohammad Iqbal, "Defining Cyberterrorism" (2004) 22:2 J Marshall J Computer & Info L 397–408 at 407.

[276] For example, Robert Diab argues that compelled third party decryption could be necessary to prevent terrorism and other serious offences, in what he calls the "national security and ticking time bomb hypotheticals." Diab, *supra* note 3 at 269–270. See also Jaffer & Rosenthal, *supra* note 101; Manpearl, *supra* note 2; Lowell, *supra* note 221.

[277] The source of this obligation is related to the origins of criminal law. For different theories about these origins, see most importantly Thomas Hobbes, *Leviathan: Or the Matter, Forme and Power of a Commonwealth Ecclesiasticall and Civil* (1651); John Locke, *Second Treatise of Government* (Awnsham Churchill, 1689); Jean-Jacques Rousseau, *Du Contrat Social, ou Principes du Droit Politique* (1762); Hans Kelsen, "Droit et état du

As Karen G. Lowell puts it, "[e]ncryption is not only a national security issue, however, as it also affects local law enforcement's ability to solve criminal cases."[278] Advocates for broader compulsory powers will argue that security is at risk when encryption is implemented in such way that the state is unable to access data relevant to an investigation, even with the appropriate court orders.

Encryption can indeed halt a criminal investigation.[279] As mentioned, this scenario was suggested by the government of Canada as part of the 2016 nationwide public safety consultation,[280] and examples where investigations were actually slowed down or stalled because of encryption were referred to by the CACP in their 2016 resolutions.[281] Nonetheless, the consultations revealed that respondents were generally against restricting encryption capacities in the name of efficient law enforcement or security.[282]

While some say that the "going dark" problem might be overstated because traditional investigations methods are still available to law enforcement,[283] and because we live in a golden age of surveillance,[284] it is accurate to state that in some cases, police will be unable

point de vue d'une théorie pure" (1936) 2 Annales de l'Institut Droit Comparé de l'Université de Paris 17; but also contemporaries such as Lindsay Farmer, *Making the modern criminal law: criminalization and civil order* (Oxford, United Kingdom: Oxford University Press, 2016); Malcolm Thornburn, "Criminal Law as Public Law" in RA Duff & Stuart Green, eds, *Philos Found Crim Law* (Oxford ; New York: Oxford University Press, 2011) 543.

[278] Lowell, *supra* note 221 at 486.

[279] See Section 2.1 of previous chapter.

[280] Public Safety Canada, *supra* note 79 at 61.

[281] Canadian Association of Chiefs of Police, *supra* note 87.

[282] Public Safety Canada, *supra* note 83.

[283] Opderbeck, *supra* note 3 at 1661–1663; Folkinshteyn, *supra* note 141 at 407.

[284] Swire & Ahmad, *supra* note 39 at 463 and following; Hurwitz, *supra* note 69 at 400–401; Phillip Rogaway, *The Moral Character of Cryptographic Work* (Auckland, New Zealand, 2015) at 26; Rozenshtein, *supra* note 35 at 1200; *Human Rights and Encryption*, by Wolfgang Schulz & Joris Van Hoboken, Series on Internet Freedom (France: UNESCO, 2016) at 24.

to access data relevant to their investigation due to strong encryption technology. According to Diab, even if we consider the alternative investigation techniques that law enforcement can employ in order to access the relevant data, law enforcement could be unable to respond in a timely fashion or these alternatives may be too costly to be used regularly by the state.[285]

A more marginal way of defining security in this sphere is to see it on a more individual level. Security is then described as what Michael Froomkin and Zak Colangelo name "safety," which is the ability to protect one's bodily integrity, livelihood, and possessions, from harm, or threat, or diminishment.[286] According to this perspective, privacy and safety are not opposed, quite the contrary. Privacy is seen as furthering safety, as "(1) it makes one physically safer; (2) it provides psychological security; (3) it makes one economically safer (and protects from some forms of invidious discrimination); and (4) it makes the exercise of various political rights safer."[287] This new rhetoric—one that does not oppose security to privacy—is gaining more and more traction and is increasingly being perceived as a way of balancing these seemingly irreconcilable interests.

3.3 Striking the Balance Between the Two

The idea that privacy is opposed to the interest of the state is not new. Indeed, John Locke and John Stuart Mill both recognized that privacy entails excluding governmental authority

[285] Diab, *supra* note 3 at 284.
[286] Froomkin & Colangelo, *supra* note 254 at 154.
[287] *Ibid* at 163. See also Moore, *supra* note 240 at 205–206 who states that: "[a]t the most basic level security affords individuals controls over their lives, projects, and property. To be secure at this level is to have sovereignty over a private domain—it is to be free from unjustified interference from other individuals, corporations, and governments."

from personal affairs.[288] This duality is also reflected in s. 8 of the *Charter* and its American counterpart, the Fourth Amendment, which both aim to balance the state's interest in investigating and prosecuting crime with citizens' privacy interests. Liberal communitarian philosophy puts this duality at the center of its theory and accepts that national security and individual privacy are two "fully legitimate normative and legal claims… and that neither can be maximized nor fully reconciled, as there is an inevitable tension between these two claims."[289] Alan Westin also opposed the two values more than 50 years ago.[290]

Around the same time that Westin was carving out his theory on privacy, which would later on become a staple of the SCC's jurisprudence on the subject,[291] Herbert L. Packer, from Yale Law School, was crafting his own models of the criminal process. He did this in a manner that recognizes the tension between privacy and security and encompassed this duality in two opposed models: the 'Due Process Model' and the 'Crime Control Model.'[292] On one side, the 'Due Process Model' aims to limit coercive state powers, in the aims of protecting individual rights (including the right to privacy); on the other, the 'Crime Control Model' presupposes that the repression of criminal conduct is the most important function of the criminal justice process, thus justifying the existence of important coercive powers. In Packer's own words:

---

[288] Molitorisz, *supra* note 232, referring to John Locke's 1689 "Second Treatise on Government" and John Stuart Mill's 1859 essay "On Liberty".
[289] Etzioni, *supra* note 25 at 569.
[290] Westin, *supra* note 239 at 7.
[291] *Spencer*, *supra* note 241 at para 40; *R v Dyment*, [1988] 2 SCR 417 at 427 [*Dyment*]; *Jarvis II*, *supra* note 263 at para 66; *Edwards*, *supra* note 235 at para 61; *Tessling*, *supra* note 250 at para 23; *Cole*, *supra* note 30 at para 42; *Marakah*, *supra* note 260 at para 39; *R v Gomboc*, 2010 SCC 55 [2010] 3 SCR 211 at para 19 [*Gomboc*]; *Mills II*, *supra* note 264 at para 98; *R v Quesnelles*, 2014 SCC 46, [2014] 2 SCR 390 at para 34; *R v Le*, 2019 SCC 34, [2019] 2 SCR 692 at para 221.
[292] Herbert L Packer, "Two Models of the Criminal Process" (1964) 113 U Pa L Rev 1.

> A totally efficient system of crime control would be a totally repressive one since it would require a total suspension of rights of privacy. We have to be prepared to pay a price for a regime that fosters privacy and champions the dignity and inviolability of the individual. That price inevitably involves some sacrifice in efficiency; consequently, an appeal to efficiency alone is never sufficient to justify any encroachment on the area of human freedom.[293]

While Packer's theory has not been unanimously well received by commentators[294] and is only one of the models that have been suggested regarding the ambit of the state's coercive powers,[295] Packer's polarization of the criminal justice system is clearly embodied in the encryption debate and its reliance on the 'security versus privacy' rhetoric. Generally, striking the balance between security and privacy has grown to be central to the debate about implementing new police and security powers in western democracies.[296] However, finding equilibrium between these seemingly opposed concepts has proven to be especially difficult in the context of encryption. As presented by Jaffer and Rosenthal:

---

[293] *Ibid* at 27.

[294] See *inter alia* Kent Roach, "Four Models of the Criminal Process" (1999) 89:2 J Crim L & Criminology 671; Stuart MacDonald, "Constructing a Framework for Criminal Justice Research: Learning from Packer's Mistakes" (2008) 11:2 New Crim L Rev 257; Peter Arenella, "Rethinking the Functions of Criminal Procedure: The Warren and Burger Courts' Competing Ideologies" (1983) 72 Geo LJ 185; Erik Luna, "A Place for Comparative Criminal Procedure" (2003) 42 Brand LJ 277; Abraham S Goldstein, "Reflections on Two Models: Inquisitorial Themes in American Criminal Procedure" (1974) 26 Stan L Rev 1009.

[295] See *inter alia* Roach, *supra* note 294; John Griffiths, "Ideology in Criminal Procedure or a Third Model of the Criminal Process" (1970) 79 Yale LJ 359; MacDonald, *supra* note 294; Keith Findley, "Toward a New Paradigm of Criminal Justice: How the Innocence Movement Mergers Crime Control and Due Process" (2008) 41 Tex Tech L Rev 133.

[296] Especially after the 9/11 terrorist attacks, which really changed the narrative regarding the importance of surveillance for national security. See Geoffrey S Corn, "Encryption, Asymmetric Warfare, and the Need for Lawful Access" (2017) 26:2 Wm & Mary Bill Rts J 337 at 354–355; Diab, *supra* note 3 at 268; Etzioni, *supra* note 25 at 582; Gill, Israel & Parsons, *supra* note 3 at 65; Jaffer & Rosenthal, *supra* note 101 at 279–280 citing Carroll Doherty, "Balancing Act: National Security and Civil Liberties in Post-9/11 Era" 2013 Pew Res. Ctr. "(stating that generally since 9/11, Americans have valued national security over their civil liberties.);" Lowell, *supra* note 221 at 498; *Don't Panic: Making Progress on the "Going Dark" Debate*, by Jonathan L Zittrain et al (The Berkman Center for Internet & Society at Harvard University, 2016) at Appendix 1, 1.

> Because security means very little without privacy, and vice versa, the current debate—which is polarized between those who claim that government access to encrypted communications is either impossible or will destroy both security and privacy on the Internet and those who claim that a lack of access to such data will mean that the government "goes dark," essentially flying blind while trying to stop active threats—is vastly un-helpful and highly unlikely to reach a stable result.[297]

The stalemate between security and privacy in the encryption debate is in part due to the limitations inherent in the technology itself. Multiple advocates against compelled decryption argue that, apart from creating the potential for state invasion of privacy, inserting some type of key-escrow or backdoor access that could be used by law enforcement would necessarily create a vulnerability in the software or hardware that could be used by criminals and generally put personal data at risk.[298] Thus, any policy on compelled decryption needs to recognize the potential risk of adopting such measure, as well as the technical capacities of TPDCs. Indeed, unlike most technologies analyzed by the courts in recent years, such as FLIR technology,[299] mobile device identifiers (MDI),[300] or computer searches in general,[301] decisions about compelled decryption could mean imposing burdensome obligations on

---

[297] Jaffer & Rosenthal, *supra* note 101 at 277.

[298] Abelson et al, *supra* note 3 at 3; Gerald Chan & Stephen Aylward, "FBI v. Apple and beyond: Encryption in the Canadian Law of Digital Search and Seizure" (2016) 1:1 J Data Protection & Priv 2 at 15; Chen, *supra* note 3 at 194; James Czerniawski & Connor Boyack, "Reviewing the Privacy Implications of Law Enforcement Access to and Use of Digital Data" (2021) 5:1 Utah J Crim L 73 at 83; Dheri & Cobey, *supra* note 77 at 4; Pratik Prakash Dixit, "Conceptualising Interaction between Cryptography and Law" (2018) 11:3 NUJS L Rev 327 at 346; Hurwitz, *supra* note 69 at 412–414; Kerr & Schneier, *supra* note 22 at 1006; Lear, *supra* note 72; Opderbeck, *supra* note 3 at 1663; Penney & Gibbs, *supra* note 3 at 220; Potapchuk, *supra* note 138 at 1411; Swire & Ahmad, *supra* note 39 at 433.

[299] *Tessling*, *supra* note 250.

[300] *R c Mirarchi*, 2015 QCCS 6628 [*Mirarchi I*]; *R v Brewster*, 2016 ONSC 4133; *R v Jennings*, 2018 ABQB 296; *X (Re)*, 2017 FC 1047.

[301] *Vu*, *supra* note 1; *Morelli*, *supra* note 30; *Cole*, *supra* note 30.

TPDCs, as they would need to modify their software or develop new types of encryption in order to respond to these requests, if that is even possible.[302]

On the other side, the argument that the only solution to preserve computer and data security is a complete ban on compelled decryption does little to balance opposing interests. Refusing to adopt any compelled decryption powers, whether imposed on individuals or on TPDCs, creates "impenetrable zones of privacy,"[303] which is inconsistent with the current jurisprudence on s. 8 of the *Charter*. On numerous occasions, the courts have stated that the constitutional protection of privacy does not grant individuals a right to absolute privacy, as privacy may give way to other important state objectives, such as law enforcement.[304]

The criminal justice system, in its rules, also aims to promote the rule of law and to uncover the truth of a case.[305] Compelled decryption can be seen as furthering these valid state interests. *A contrario*, using privacy as an argument against such state power can be seen as harmful to the public good because it "would prevent exposure of truthful information."[306] As George Dolhai presents it, the state's investigative powers must not only focus on proving someone's guilty but also on finding the true perpetrator of the crime, so that they can be

---

[302] This, among other reasons that will be analyzed in Chapter 8, militates for rapid legislative action, rather than waiting for the courts to decide on this issue.

[303] Corn, *supra* note 296 at 345. See also Lowell, *supra* note 221 at 503–504 to the same effect.

[304] Most importantly in *Hunter*, *supra* note 31 at 159–160; *Gomboc*, *supra* note 291 at para 46; *R v O'Connor*, [1995] 4 SCR 411 at para 117.

[305] Diab, *supra* note 3 at 269.

[306] Froomkin & Colangelo, *supra* note 254 referring to Heidi R Anderson, "The Mythical Right to Obscurity: A Pragmatic Defense of No Privacy in Public" (2012) 7 JL Pol'y Info & Soc 543. On the truth seeking function of criminal procedure, see generally Packer, *supra* note 292; Arenella, *supra* note 294; Mirjan Damaska, "Evidentiary Barriers to Conviction and Two Models of Criminal Procedure: A Comparative Study" (1973) 121 U Pa L Rev 506; Donald A Dripps, "The Substance-Procedure Relationship in Criminal Law" in RA Duff & Stuart Green, eds, *Philos Found Crim Law* (New York: Oxford University Press, 2013); John D Jackson, "Theories of Truth Finding in Criminal Procedure: An Evolutionary Approach" (1988) 10 Cardozo L Rev 475.

prosecuted and convicted.[307] Accordingly, aiming to find the truth of a case also implies sparing the innocent from wrongful convictions,[308] which is a well-known preoccupation of criminal law.[309]

Jeremy Bentham is perhaps the leading theorist that has focused on the search for truth as a central value of the justice system. For Bentham, some procedural rules are indeed justified by the fact that they "[provide] means of coming at the truth,"[310] including rules that provide law enforcement with search and seizure powers. According to his vision, procedural rules are only meant to serve the corresponding substantive law's goal and to further the search for the truth of a case. As he saw criminal law's objectives as being the "control [of] socially harmful behaviour [and the reduction of] mischief,"[311] criminal procedural rules should then strive to do the same.[312] Accordingly, Bentham was reticent to limit the collection or use of

---

[307] Dolhai, *supra* note 250 at 7. Dolhai also refers to the SCC in *CanadianOxy Chemicals Ltd v Canada (Attorney General)*, [1999] 1 SCR 743 at para 19, in which the Court states that individual privacy must sometimes give way to the public interest in prompt and thorough criminal investigations.

[308] Dolhai, *supra* note 250 at 7.

[309] On the idea that criminal law must aim to protect the innocent, see generally Jeremy Bentham, "Principles of Judicial Procedure with the Outlines of a Procedure Code" in John Bowring, ed, *Works Jeremy Bentham* (Edinburgh: William Tait, 1843); Packer, *supra* note 292; Susan A Bandes, "Protecting the Innocent as the Primary Value of the Criminal Justice System" (2009) 7 Ohio St J Crim L 413; Arenella, *supra* note 294.

[310] Bentham, *supra* note 309 at 15.

[311] Jeremy Bentham, "An Introduction to the Principle of Morals and Legislation" in JH Burns & HLA Hart, eds, (London: Methuen, 1970), as cited in Gerald J Postema, "The Principle of Utility and the Law of Procedure: Bentham's Theory of Adjudication" (1977) 11 Ga L Rev 1393 at 1395.

[312] At lot could be said here about the diverging opinions about the aims of criminal law. Multiple theories have been suggested over the years about the goals of criminal law: retributivism, consequentialism, liberalism, instrumentalism, utilitarianism… While a complete thesis could be dedicated to this subject, suffice to say here that the goal of criminal law has been described by the SCC as being "the public identification of wrongdoing *qua* wrongdoing which violates public order and is so blameworthy that it deserves penal sanction." See *R v Mabior*, 2012 SCC 47, [2012] 2 SCR 584 at para 23. This short statement encompasses various elements that are part of theories suggested over the years, such as the fact that criminal law is partly justified by an underlying concept of morality. By including the notion of sanction, the SCC also recognizes that criminal law is concerned with punishment, at least to some degree, which is aligned with a retributivist perspective. On retributivism, see *inter alia* Stephen R Galoob, "Retributivism and Criminal Procedure" (2017) 20:3 New Crim L Rev 465; Michael S Moore, Placing Blame: A General Theory of the Criminal Law (Oxford: Oxford University Press, 2010); Darryl K Brown, "Criminal Law Theory and Criminal Justice Practice" (2012) 49 Am Crim L Rev 73;

relevant evidence, as evidence is necessary to discover the truth and to ultimately reach a correct decision.[313] From a Benthamite utilitarian perspective then, compelled decryption would most likely be easily accepted, as an investigative technique that furthers the search for the truth of a case.

Recognizing that the state has an obligation to investigate and prosecute crimes and to uncover the truth of a case, however, does not mean that the state has *carte blanche* to implement any method of investigating the crimes committed on its territory, nor that it has the right to the most efficient investigation techniques.[314] Indeed, our adversarial criminal justice system allows for multiple values to compete.[315] Bentham's adjective law theory, by focusing so heavily on the search for truth, is famous for not making room for due process considerations,

---

Arnulf Zweig, "Retributivism, Resentment and Amnesty" (1995) 3 Jahrb Recht Ethik 267; Michael T Cahill, "Retributive Justice in the Real World" (2007) 85 Wash U L Rev 815. Generally speaking, contemporary theorist Lindsay Farmer's perspective on the aim of criminal law seems very much in line with the SCC's jurisprudence on criminal law and the choices that have been made in this regard in Canada. Farmer, from the University of Glasgow, sees criminal law as securing civil order, by creating norms that guide or shape individual conduct. As such, civil order is not only a precondition to the existence of law, as postulated by John Locke, but also a consequence of its existence. See Lindsay Farmer, *supra* note 277.

[313] Bentham, *supra* note 309 at 3 and 5. As put by Bentham himself: "Let in the light of evidence. The end it leads to, is the direct end of justice, rectitude of decision." Jeremy Bentham, "On Exclusion of Evidence" in John Bowring, ed. *Works of Jeremy Bentham* (Edinburgh: William Tait, 1843) at 336.

[314] This is maybe most clear when considering that the *Charter* in itself aims to limit governmental action and to promote individual rights and freedoms, not create police power or enable governmental action. As put very eloquently by Dickson J. in *Hunter*, *supra* note 31 at 157:

> I begin with the obvious. The *Canadian Charter of Rights and Freedoms* is a purposive document. Its purpose is to guarantee and to protect, within the limits of reason, the enjoyment of the rights and freedoms it enshrines. It is intended to constrain governmental action inconsistent with those rights and freedoms; it is not in itself an authorization for governmental action. In the present case this means, as Prowse J.A. pointed out, that in guaranteeing the right to be secure from unreasonable searches and seizures, s. 8 acts as a limitation on whatever powers of search and seizure the federal or provincial governments already and otherwise possess. It does not in itself confer any powers, even of "reasonable" search and seizure, on these governments. This leads, in my view, to the further conclusion that an assessment of the constitutionality of a search and seizure, or of a statute authorizing a search or seizure, must focus on its "reasonable" or "unreasonable" impact on the subject of the search or the seizure, and not simply on its rationality in furthering some valid government objective.

[315] As opposed to inquisitorial systems which are seen as generally favoring the search for truth as their central value. See John D Jackson, *supra* note 306; Damaska, *supra* note 306.

thus privacy considerations,[316] which is inconsistent with Canadian criminal law.[317] In that sense, it has been said that "[s]ociety's commitment to privacy often entails restraining or even sacrificing interests of substantial importance, such as … efficient law enforcement."[318] Because law enforcement does not have a constitutional right to have access to the most efficient methods, it will necessarily have to satisfy itself with techniques that are deemed reasonable, when balanced with the individual right to privacy.

The choice between these interests not only depends on technical or constitutional considerations but also on the resources of lobbying entities, the values favored by the political party in office, and the social climate that prevails at a specific point in time. As Colton Fehr points out, lobbying groups in Canada, whether civil rights groups or telecommunications service providers, have in the past successfully halted Parliament from adopting specific policies.[319] Cryptography, which encryption is a subset of, is inherently political and linked to power.[320] Regulating it and controlling it thus raise fundamental questions about what values we want to promote as a society.[321]

The government of Canada has in the past presented the privacy versus security debate in a way that demonizes encryption and effectively politicizes this issue. In 2019, the Minister of

---

[316] See for example William Twining, "Evidence and Legal Theory" (1984) 47:3 Mod L Rev 261.
[317] Dripps, *supra* note 306, classifies systems as being 'rationalist' or 'pluralist,' where the former focus on truth-finding as the central value of the criminal process and the latter allow for multiple values to compete in the criminal process. Following this classification, Canada would be a 'pluralist' system.
[318] Daniel J Solove, "Conceptualizing Privacy" (2002) 90 Calif L Rev 1087 at 1093–1094, cited in Froomkin & Colangelo, *supra* note 254 at 161–162. To the same effect, see Vassilaki, *supra* note 270 at 42.
[319] Colton Fehr, "Criminal Law and Digital Technologies: An Institutional Approach to Rule Creation in a Rapidly Advancing and Complex Setting" (2019) 65:1 McGill LJ 67 at 102–105.
[320] Rogaway, *supra* note 285; Derek E Bambauer, "Privacy versus Security" (2013) 103:3 J Crim L & Criminology 667 at 673.
[321] Bambauer, *supra* note 320 at 673.

Public Safety and Emergency Preparedness, the Honourable Ralph Goodale, talked about encryption in a way that made it seem like encryption only serves child abusers, as did his predecessor Vic Toews.[322] This type of rhetoric does little to further the debate about encryption and makes it difficult for most citizens to have a nuanced opinion about the subject. It fails to recognize the positive values of encryption and the fact that the government itself benefits from strong encryption when it comes to protecting itself from unwanted intrusions.

Privacy is also often contrasted with a "nothing to hide" rhetoric, in the sense that some people do not care about their personal spaces being invaded because they are not participating in any unlawful activity and thus do not worry about the government collecting or analyzing data that concerns them, as it is benign or at most embarrassing. Daniel J. Solove calls it "one of the primary arguments made when balancing privacy against security," and one that makes it difficult for privacy to prevail.[323] This point of view, while possibly relevant to assessing the value that a specific person gives to privacy, fails to consider that measures restricting the state's compulsory powers on its citizens not only protects privacy but also serve as a safeguard against an overreaching or totalitarian state.[324] Accepting the rhetoric would mean that privacy's only value "is about hiding a wrong."[325] It fails to consider the positive aspects

[322] Parsons, *supra* note 56 at 4.

[323] He also cites Bruce Schneier and Geoffrey Stone that respectively refers to this discourse as the "most common retort against privacy advocates" and an "all-too-common refrain." Solove, *supra* note 251 at 747 and 752.

[324] Moore, *supra* note 240 at 202–204.

[325] Bruce Schneier, "The Eternal Value of Privacy", (18 May 2006), online: *Wired* <https://www.wired.com/2006/05/the-eternal-value-of-privacy/#:~:text=Privacy%20is%20an%20inherent%20human,%22Absolute%20power%20corrupts%20absolutely.%22> cited in Solove, *supra* note 251 at 764.

of privacy, such as enabling freedom of expression and opinion,[326] and encouraging human flourishing.[327]

In a 2007 article on the technological advances in surveillance technology, Arthur J. Cockfield suggested that reframing privacy to acknowledge its social value is necessary to evaluate if the use of certain technologies by law enforcement or intelligence officials should be allowed. He lists six adverse effects that increased surveillance can have on the social value of privacy:

> increased scrutiny by state agents can: (a) stifle political dissent as individuals fear reprisal by government actors; (b) inhibit freedom of expression as individuals fear public scrutiny of their views or behavior; (c) lead to racial or religious profiling, that is, discrimination which targets identifiable groups despite no evidence of individual wrong-doing; (d) have a disproportionately adverse impact on lower income Canadians who tend to make greater use of public spaces, which are increasingly subjected to state scrutiny; (e) result in political complacency to the extent that ubiquitous surveillance eliminates any subjective expectation of privacy and discourages citizens from questioning more and more state scrutiny; and (f) make it harder to hold state agents accountable for their potentially abusive behavior in part because of the surreptitious nature of the new technologies.[328]

These concerns can be applied *mutatis mutandis* to the type of surveillance that could be enabled following a weakening of available encryption. In turn, the erosion of the social value of privacy would make the Canadian public less secure, rather than the other way around.[329] As digital communications technologies become more and more pervasive in all aspects of

[326] Kaye, *supra* note 112.
[327] Froomkin & Colangelo, *supra* note 254 at 146–147.
[328] Cockfield, *supra* note 253 at 4–5.
[329] *Ibid* at 5.

people's lives, the "traditional privacy/security dialectic [is proving to be] unhelpful,"[330] to say the least.

Reframing the dichotomy between security and privacy is maybe the best way to resolve this impasse. If we construct security in a different manner, privacy and security are not competing interests, quite the contrary. Indeed, when it comes to computer and data security, strong encryption capacities positively impact privacy because encryption protects data from unwanted intrusions.[331] Put in another way, "security implements privacy."[332] Interpreted in this manner, national security is furthered with strong encryption, as encryption does not only protect citizens against unwanted access from hackers or law enforcement, but also protects the state from the same unwanted access.[333] As Moore puts it:

> National security for government agencies, companies, and individuals actually *requires* strong encryption. Spies have admitted to "tapping in" and collecting valuable information on U.S. companies—information that was then used to gain a competitive advantage. A report from the CSIS Task Force on Information Warfare and Security notes that "cyber terrorists could overload phone lines . . . disrupt air traffic control . . . scramble software used by major financial institutions, hospitals, and other emergency services . . . or sabotage the New York Stock Exchange." Related to information war, it would seem that national security requires strong encryption, multilevel firewalls, and automated detection of attacks.[334]

---

[330] *Ibid* at 4.

[331] As Zarefsky, puts it: "The primary catalyst for the data security of modern smartphones, tablets, and computers is encryption technology." See Jacob Zarefsky, "The Precarious Balance between National Security and Individual Privacy: Data Encryption in the Twenty-First Century" (2021) 23 Tu J Tech & Intell Prop 179.

[332] Bambauer, *supra* note 320 at 671.

[333] Moore, *supra* note 240 at 208–209.

[334] *Ibid* (references omitted).

Recognizing that privacy and security can be, or at least need to be, reconciled when it comes to national security drives the conclusion that the encryption problem in criminal investigations will need to be resolved without limiting encryption capabilities unduly, if at all. On the contrary, any policy regulating encryption cannot exist in a vacuum of what encryption technology is effectively capable of protecting, at a cost we are willing to accept.[335]

Further, if we follow Michael Froomkin and Zak Colangelo's safety as security model, encryption can be a method of protecting communicational privacy, which provides "safety" (or individual security) for individuals.[336] Considered this way, "it would seem privacy and security come bundled together."[337] By accepting that both concepts can coexist, we can finally move on from the standstill that is currently inhibiting any constructive dialogue around encryption.

Reconciling privacy and security is not impossible; it depends on the definitions we give to these concepts and the practical application of those definitions. Strong encryption (as well as other measures that enhance privacy, such as authentication[338]) should be contrasted to efficient law enforcement, rather than security, as encryption not only benefits individuals but also the government. Thus, opposing privacy and security in the encryption debate—which inevitably opposes the government to the individual—fails to recognize that encryption is essential in the current digital world we live in.

---

[335] Bambauer, *supra* note 320 at 677–678.

[336] Froomkin & Colangelo, *supra* note 254 at 184.

[337] Moore, *supra* note 240 at 205–206.

[338] The term authentication refers in computing to "the process of verifying the identity of a person or device." TechTerms, "Authentication", (2018), online: *TechTerms* <https://techterms.com/definition/authentication>; Bambauer, *supra* note 320, referring to Jon L. Mills, Privacy: The Lost Right, Oxford: Oxford Scholarship Online (2008).

By focusing on the individual interest in privacy as being opposed to society's interest in effective law enforcement, this thesis proposes a framework that allows for compelled decryption, in very specific situations, using court orders, rather than directly by police officers. This framework works under the postulate that compelled unlocking of devices or compelled decryption of data does not necessarily infringe ss. 7 rights and 8 rights, if specific circumstances are present and strict conditions are put in place. Alternatively, the framework could be justified under s. 1 of the *Charter* and the *R v Oakes* test, if compelled decryption is determined to violate the *Charter*.[339] Furthermore, and as it will be explained more thoroughly in the following chapters, the limits of the principles of fundamental justice also entail harmonizing opposed interests and achieving a balance between individual rights and the state's obligation to investigate and prosecute crime. Therefore, the opposed interests at play when it comes to encryption will strongly influence the framework proposed in this thesis.

Reframing the debate in the manner discussed above seems to calm the tensions between opposed polarities present in the criminal justice system, as it recognizes that privacy, implemented by encryption, can be beneficial to security and to the collective interest in preventing unwanted access to both individual- and state-owned data, while also considering that law enforcement does not have a right to the most efficient investigative techniques, but rather it must be limited to techniques that properly accommodate the privacy interests at play, within the scope of how they are protected by law. The necessity of harmonizing collective and individual rights is not a new idea, as Adam Smith himself postulated that civil and

[339] See Liam M Hayes, "Smartphone Searches: A Legal Crossroads Between *Charter* Rights and Law Enforcement" (2018) 66 Crim LQ 196 at 11-12 and also Chapter 7, *infra*.

individual interests are intertwined.[340] As put by Farmer, Adam's writings on the justification of civil government show that "in the conflation of the individual and the social interest, civil order [is] to be secured through the securing of individual interests."[341]

[340] Adam Smith, *Lectures on Jurisprudence* (Oxford: Oxford University Press 1978), cited in Farmer, *supra* note 277 at 59.
[341] Farmer, *supra* note 277 at 59.

CHAPTER 4 THE RIGHT AGAINST SELF-INCRIMINATION

In their search for the truth of a case, law enforcement will necessarily aim to gather as much relevant evidence as possible, using the different methods at their disposal, such as search warrants, production orders, or common law search powers. Traditionally, considerations about the legality of law enforcement's gathering of evidence, specifically with regard to real/physical evidence, were considered under s. 8 of the *Charter*. However, this is changing due to strong encryption technology and the growing fear that important evidence will evade law enforcement—and ultimately the courts—even if it was obtained in a manner that respects s. 8 of the *Charter*. As Nicola Dalla Guarda puts it:

> … the most pressing concern on the horizon for Canadian criminal law will not be found in academic debates and shifting judicial interpretations over privacy and the "right to be secure against unreasonable search or seizure" enshrined in the *Charter of Rights and Freedoms* (*Charter*). Rather, criminal activity conducted in or through the digital realm will soon make use of powerful and accessible encryption technology in order to evade investigation and prosecution. This, in turn, will generate far more profound questions regarding the right to be free from self-incrimination, which has been recognized for centuries in the common law and is today protected by various sections of the *Charter* as a "principle of fundamental justice" central to the criminal justice system as a whole.[342]

[342] Dalla Guarda, *supra* note 32 at 120.

The right, or protection, [343] against self-incrimination as a principle of fundamental justice protected by s. 7 of the *Charter* plays an important role in Canadian criminal law,[344] *inter alia* because it provides protection for interests such as privacy, dignity and autonomy of the person.[345] As an overarching principle justifying numerous rules, such as the right to silence, the privilege against testimonial self-incrimination and the right of the accused to not be compelled as a witness, the principle against self-incrimination will indeed prove important when it comes to determining if a police power to compel decryption or unlocking of devices can be authorized under the *Charter* and, if so, under what conditions.

In order to examine how the principle against self-incrimination can come into play when it comes to compelled decryption, this chapter will provide the necessary foundations for the ongoing analysis. It will examine the origins and the underlying *raisons d'être* of the principle and the numerous rules it justifies and supports. The analysis suggested in this chapter is fairly extensive and chronological. This was done having in mind that the principle against self-incrimination has generally received less attention in recent years than the protection against unreasonable search and seizure, especially when it comes to its applicability to the obtention of electronic evidence. It is also done to demonstrate that the application of the principle against self-incrimination has prompted contrasting results in different situations, making it

[343] The terms "principle" or "right" against self-incrimination are used to distinguish the overarching principle against self-incrimination from its subset "privilege" afforded to witnesses in investigative proceedings. See dissenting reasons by Lamer J. in *R v Jones*, [1994] 2 SCR 229 [*Jones I*] (now considered authoritative because endorsed by the majority in *R v S (RJ)*, [1995] 1 SCR 451 [*S (RJ)*]. See also Pat McInerney, "The Privilege against Self-Incrimination from Early Origins to Judges' Rules: Challenging the Orthodox View" [2014] 18 Int'l J Evidence & Proof 101 at 102.

[344] Lisa Dufraimont, "The Patchwork Principle against Self-Incrimination under the Charter" (2012) 57 SCLR (2d) 241.

[345] *Thomson Newspapers Ltd v Canada*, [1990] 1 SCR 425 at 480.

difficult to predict its application to the "going dark" problem (which will be done subsequently in Part II) with absolute certainty.

4.1 The Evolution of the Principle Against Self-Incrimination in Canadian Criminal Law

4.1.1 Prior to the Adoption of the Canadian Charter of Rights and Freedoms

Originally, the term "self-incrimination" (or sometimes "self crimination"[346]) was associated with testimonial compulsion at the trial stage of the criminal process. According to Ed Ratushny, whose 1973 article was cited multiple times by the SCC, "the concept of self-incrimination is not applicable at all to the pre-trial stage."[347] According to Ratushny, the pre-trial right to silence (which is now linked with the overarching protection against self-incrimination and the subset privilege against self-incrimination[348]) was rather rooted in the principle of the rule of law, and not into any concept of self-incrimination. This understanding of the right to silence was shared by the SCC in *Rothman v R*, prior to the advent of the *Charter*.[349] Put differently, because there is no obligation to assist or aid law enforcement in Canadian criminal law, individuals have a right to remain silent.

---

[346] As in the *Canadian Bill of Rights*, SC 1960, c 44 at para 2(d), in the *Charter*, *supra* note 24, s 13, or in older cases such as *Curr v R*, [1972] SCR 889, but also more recent cases. See for example *R c McGown*, 2016 ONCA 575; *R v Bishop*, 2002 NSPC 2. However, authors, lower court decisions, and the Supreme Court jurisprudence on the subject strongly favor the term "self-incrimination."

[347] Ed Ratushny, "Is There a Right against Self-Incrimination in Canada?" (1973) 19:1 McGill LJ 1 at 9.

[348] See Section 4.2.2. *infra.*

[349] *Rothman v R*, [1981] 1 SCR 640 at 683 per Lamer J (dissenting).

SCC decisions *Curr*[350] and *Marcoux & Solomon*[351] demonstrate that self-incrimination was perceived in a very limited manner prior to the advent of the *Charter*. Until that point, self-incrimination only provided limited protection to witnesses, as it was held that no general or residual protection against self-incrimination existed, whether in the common law or in the *Canadian Bill of Rights*.[352]

This testimonial protection against self-incrimination afforded to witnesses (including the accused) is also called *privilege* against self-incrimination. In common law, the privilege is expressed by "the confessions rule, the right to silence, and rules protecting witnesses from the use of their testimony against them in other proceedings,"[353] all of which are concerned with testimonial evidence only. These protections are said to have been created in response to "the abhorrence of the coercive "Star Chamber" practises which characterized English justice as late as the 16th century."[354] However, not everyone agrees with the exact origins of this distaste for compelled self-incriminatory testimony,[355] or the necessity to establish them with absolute certainty.[356] Regardless, what is clear is that common law has historically included different rules that protect witnesses and the accused from forced testimony at trial, including the right to refuse to answer questions that might incriminate oneself, a rule that still prevails in the United States by way of the Fifth Amendment.

---

[350] *Curr*, *supra* note 341.
[351] *Marcoux and Solomon v R*, [1976] 1 SCR 763 [*Marcoux and Solomon*].
[352] Ratushny, *supra* note 347 at 76; *Marcoux and Solomon*, *supra* note 351 at 769; *Curr*, *supra* note 341 at 913.
[353] *R v Stillman*, [1997] 1 SCR 607 at para 200 [*Stillman*] (McLachlin J., dissenting).
[354] *Ibid*; *Thomson Newspapers Ltd v Canada*, *supra* note 345 at 471, 477; Fariborz Davoudi, "The Privilege Against Self-Incrimination (Part III)" (2017) RegQuest at 1; Kiel Walker, "La protection contre l'auto-incrimination testimoniale au Canada et le droit québécois: Quoi protège qui?" (2015) 46:2 Ottawa L Rev 315 at 3; Wiseman, *supra* note 6 at 536–537; *R v Henry*, 2005 SCC 76, [2005] 3 SCR 609 at para 2 [*Henry*].
[355] McInerney, *supra* note 343.
[356] *S (RJ)*, *supra* note 343.

Canada, however, veered off from the traditional common law rule on compelled self-incrimination during the trial phase of the criminal proceedings by adopting, in 1893, what is now s. 5 of the *Canada Evidence Act* and subsequently in 1982 by adopting s. 13 of the *Charter*.[357] Instead of allowing a witness to refuse to answer a question on the ground that it would tend to incriminate them, these rules grant witnesses use immunity—under certain conditions that will be analyzed in this chapter—except in cases of prosecution for perjury.

4.1.2 After the Adoption of the Canadian Charter of Rights and Freedoms

A) Establishing the Principle Against Self-Incrimination as a Principle of Fundamental Justice

Constitutionalizing the abandonment of the common law rule of allowing a witness to refuse to answer a question on the grounds of potential self-incrimination is not the only impact the *Charter* had on the Canadian understanding of self-incrimination. The judicial interpretation of the *Charter*, especially by Justice Lamer, has led to a dramatic overhaul of how self-incrimination is perceived by criminal law.[358] From a protection limited to testimonial

[357] *Thomson Newspapers Ltd v Canada*, *supra* note 345 at 474; *R v Kuldip*, [1990] 3 SCR 618 at 642 [*Kuldip*].
[358] David M Paciocco, "Self-Incrimination and the Case to Meet: The Legacy of Chief Justice Lamer" (2000) 5 Can Crim L Rev 63. In his (pre-judicial) article, David Paciocco puts Justice Lamer's concurring decision in *Rothman* as the starting point of his lineage of decisions on the subject of self-incrimination. According to the author, while Lamer's opinion expressed the conventional view that self-incrimination principles are not engaged when an accused makes a declaration to an undercover police officer, he nonetheless weaved "'conscription' theory and self-incrimination principles indirectly into the fabric of the law relating to pretrial statements, in the process recognizing a principle of 'choice' that has come to guide the development of the law of self-incrimination." The decision to not include R*othman* in the analysis of the jurisprudence on self-incrimination law in this thesis rests ultimately on the fact that *Rothman* was rendered prior to the advent of the *Charter*.

evidence at trial, the principle against self-incrimination has evolved to ground other rules of evidence, whether during the pre-trial phase of the criminal process or the trial phase.[359]

In *Dubois v R,*[360] Justice Lamer wrote about the protection against self-incrimination found in the different sections of the *Charter* and how these various protections can be seen as furthering the same goal of protecting the accused against compelled self-incrimination conceived largely. The majority, under Lamer J.'s authorship, concluded that s. 13 of the *Charter* "is a very specific form of protection against self-incrimination [that] must therefore be viewed in light of two closely related rights, the right of non-compellability and the presumption of innocence, set forth in s. 11(c) and (d) of the *Charter*."[361] These three separate rights interact and when combined they justify the concept of the "case to meet" that falls on the prosecution.[362] As such, these protections reflect the principle that "… the individual is sovereign and that proper rules of battle between government and individual require that the individual not be bothered for less than good reason and not be conscripted by his opponent to defeat himself."[363]

In *Thomson Newspapers Ltd. v Canada (Director of Investigation and Research, Restrictive Trade Practices Commission*,[364] the SCC examined whether the *Combines Investigation*

[359] Both the pre-trial and trial rules linked to the principle against self-incrimination will be analyzed here due to the fact that compelled decryption, while being an investigatory technique (thus used during the pre-trial phase), also raises questions of admissibility of the obtained evidence during the trial phase.
[360] *Dubois v The Queen*, [1985] 2 SCR 350 [*Dubois*].
[361] *Ibid* at 356.
[362] *Ibid* at 357.
[363] John Henry Wigmore, Evidence in Trials at Common Law, vol. 8, Revised by John T. McNaughton, Boston: Little, Brown & Co., 1962, cited in *Dubois* at 358.
[364] *Thomson Newspapers Ltd v Canada*, *supra* note 345.

Act[365] violated ss. 7 and 8 of the *Charter* by allowing the punishment of individuals refusing to comply with orders to appear before the Restrictive Trade Practices Commission to be examined under oath and to produce documents. The majority, as well as Lamer and Wilson JJ., dissenting, agreed that s. 7 of the *Charter* contains a residual protection against self-incrimination, in addition to what is already specifically protected by ss. 11(c) and 13.[366]

A few years later, in 1994, the SCC in *R v P (MB)*[367] examined the rules regarding the reopening of the Crown's case after the accused announced the calling of an alibi witness. Justice Lamer, writing for the majority, focused the analysis on the principle that accused individuals in the criminal justice system must not be conscripted against themselves. According to him:

> Perhaps the single most important organizing principle in criminal law is the right of an accused not to be forced into assisting in his or her own prosecution … This means, in effect, that an accused is under no obligation to respond until the state has succeeded in making out a *prima facie* case against him or her. In other words, until the Crown establishes that there is a "case to meet", an accused is not compellable in a general sense (as opposed to the narrow, testimonial sense) and need not answer the allegations against him or her.
>
> The broad protection afforded to accused persons is perhaps best described in terms of the overarching principle against self-incrimination, which is firmly rooted in the common law and is a fundamental principle of justice under s. 7 of the *Canadian Charter of Rights and Freedoms*. As a majority of this Court suggested in *Dubois v. The Queen*, [1985] 2 S.C.R. 350, the presumption of innocence and the power

[365] *Combines Investigation Act*, RSC 1970, c C-23, repealed and now replaced with *Competition Act*, RSC 1985, c C-34.
[366] *Thomson Newspapers Ltd v Canada*, *supra* note 345 at 442, 470, 537.
[367] *R v P (MB)*, [1994] 1 SCR 555 [*P (MB*].

> imbalance between the state and the individual are at the root of this principle and the procedural and evidentiary protections to which it gives rise.[368]

As such, the accused is given the right to remain silent in the face of the evidence presented by the Crown. However, once the Crown does indeed present a *prima facie* case, the accused might need to present evidence in order to avoid a conviction:

> In other words, once there is a "case to meet" which, if believed, would result in conviction, the accused can no longer remain a passive participant in the prosecutorial process and becomes—in a broad sense—compellable. That is, the accused must answer the case against him or her, or face the possibility of conviction.[369]

The same year as *P (MB)*, the Court examined the admissibility of evidence gathered during a psychiatric evaluation ordered by the court under the dangerous offender provisions of the *Criminal Code* in *Jones I*.[370] Perhaps what is the most interesting and relevant for our purposes from *Jones I* is Justice Lamer's dissent, which is now considered to be authoritative as it was endorsed by the majority one short year later in *R v S (RJ)* as reflecting the state of the law on self-incrimination in Canada.[371]

From the start, Justice Lamer in *Jones I* recognized that the status of the principle against self-incrimination was not so readily apparent, although it had previously been considered by the SCC, *inter alia* in *Thomson Newspapers*, *Dubois*, and *P (MB)*. Looking back at Wigmore's definition of the principle, which he had cited in *Dubois*, Lamer J. found that

---

[368] *Ibid* at 577–578.
[369] *Ibid* at 579.
[370] *Jones I*, *supra* note 343.
[371] *S (RJ)*, *supra* note 343 at para 46. See also *R v Fitzpatrick*, [1995] 4 SCR 154 at para 33 [*Fitzpatrick*].

> Any state action that coerces an individual to furnish evidence against him-or herself in a proceeding in which the individual and the state are adversaries violates the principle against self-incrimination. Coercion, it should be noted, means the denial of free and informed consent.[372]

After reviewing the different rules, rights, and privileges that can be traced to the principle against self-incrimination,[373] Justice Lamer concluded that the SCC had previously implicitly recognized the principle against self-incrimination as a principle of fundamental justice and that it should indeed receive this qualification. As such, any limitation of life, liberty, or security of the person that contravenes the right against self-incrimination would breach s. 7 and need to be justified under s. 1 of the *Charter.*[374] The SCC has since periodically restated that the principle against self-incrimination is a principle of fundamental justice in decisions such as *R v S (RJ)*,[375] *British Columbia Securities Commissions v Branch*,[376] *R v Jarvis*,[377] *Application under s. 83.28 of the Criminal Code (Re)*,[378] and *R v Hart*.[379]

At this point, it is important to underline the distinction between the *privilege* against self-incrimination and the *principle* against self-incrimination. The first is a strict rule relating to testimonial evidence, while the second is a principle of fundamental justice under s. 7 of the *Charter* that is a "general organizing principle of criminal law from which particular rules can be derived."[380] To limit our understanding of self-incrimination to the application of the

---

[372] *Jones I*, *supra* note 343 at 249.
[373] *Ibid.* See Section 4.2 *infra*.
[374] *Ibid* at 258.
[375] *S (RJ)*, *supra* note 343.
[376] *British Columbia Securities Commission v Branch*, [1995] 2 SCR 3 [*BC Securities*].
[377] *R v Jarvis*, 2002 SCC 73, [2002] 3 SCR 757 at para 67 [*Jarvis I*].
[378] *Application under s. 83.28 of the Criminal Code (Re)*, 2004 SCC 42, [2004] 2 SCR 248.
[379] *R v Hart*, 2014 SCC 52, [2014] 2 SCR 544 at para 176 [*Hart*].
[380] *Ibid* at 249.

privilege would render senseless multiple rules that are derived from the broader principle against self-incrimination.

Recognizing that the protection against self-incrimination is a principle of fundamental justice, however, does not mean that s. 7 provides "a broad right against self-incrimination on an abstract level…"[381] This residual protection against self-incrimination must still align itself with the Canadian vision of self-incrimination, which, as a principle of fundamental justice, aims at "a just accommodation between the interests of the individual and those of the state…"[382] The nature of the principles of fundamental justice will also vary with the context and will not grant the accused with the most favorable procedures that could possibly be imagined.[383]

The SCC in *R v Hebert* examined the admissibility of statements made by detained individuals to undercover police officers, under ss. 10(b) and 7 of the *Charter*.[384] Reminding us that the fundamental rights found in the *Charter* are capable of evolving and must receive a flexible interpretation by the courts, not one that is stuck in 1982 when the *Charter* was enacted,[385] the SCC determined that the principles of fundamental justice under s. 7 of the *Charter* may have a broader meaning than the specific rules they carry. This conclusion is also justified by the fact that principles of fundamental justice must embrace more than one specific rule, as

[381] *Thomson Newspapers Ltd v Canada*, *supra* note 345 at 538.
[382] *Ibid* at 539.
[383] *Ibid* at 539–540 referring to *R v Lyons*, [1987] 2 SCR 309 [*Lyons*]. See also Section 4.1.2(C) *in fine infra.*
[384] *R v Hebert*, [1990] 2 SCR 151 [*Hebert*].
[385] *Ibid* at 163, referring to *R v Therens*, [1985] 1 SCR 613 at 638.

they "reconcile[e] diverse but related principles."[386] This is true when it comes to the right to silence, which is related to the confessions rule and the privilege against self-incrimination.

The SCC in *Hebert* also examined the broader objective of s. 7 of the *Charter*. According to the majority, written by Justice McLachlin (as she then was):

> The *Charter* through s. 7 seeks to impose limits on the power of the state over the detained person. It thus seeks to effect a balance between the interests of the detained individual and those of the state. On the one hand s. 7 seeks to provide to a person involved in the judicial process protection against the unfair use by the state of its superior resources. On the other, it maintains to the state the power to deprive a person of life, liberty or security of person provided that it respects fundamental principles of justice. The balance is critical. Too much emphasis on either of these purposes may bring the administration of justice into disrepute—in the first case because the state has improperly used its superior power against the individual, in the second because the state's legitimate interest in law enforcement has been frustrated without proper justification.[387]

The right to remain silent, as well as other rules justified under s. 7 of the *Charter* such as the privilege against self-incrimination, must therefore reflect the equilibrium that must be respected when it comes to rules that impact the life, liberty, or security interests of individuals. The idea that principles of fundamental justice, such as the principle against self-incrimination, must be interpreted in light of individual and societal rights is also reflected in later SCC jurisprudence.[388]

---

[386] *Hebert*, *supra* note 384 at 163.
[387] *Ibid* at 180.
[388] *R v Darrach*, 2000 SCC 46, [2000] 2 SCR 443 at para 29 [*Darrach*]; *R v White*, [1999] 2 SCR 417 at para 47 [*White*]; *S (RJ)*, *supra* note 343 at 534; *R v Seaboyer; R c Gayme*, [1991] 2 SCR 577 at 603 [*Seaboyer*]; *BC Securities*, *supra* note 376 at 15.

Later, the Court specified the method to adopt when it comes to the interpretation of the principles of fundamental justice:

> Jurisprudence on s. 7 has established that a "principle of fundamental justice" must fulfill three criteria: *R. v. Malmo-Levine*, [2003] 3 S.C.R. 571, 2003 SCC 74, at para. 113. First, it must be a legal principle. This serves two purposes. First, it "provides meaningful content for the s. 7 guarantee"; second, it avoids the "adjudication of policy matters": *Re B.C. Motor Vehicle Act*, [1985] 2 S.C.R. 486, at p. 503. Second, there must be sufficient consensus that the alleged principle is "vital or fundamental to our societal notion of justice": *Rodriguez v. British Columbia (Attorney General)*, [1993] 3 S.C.R. 519, at p. 590. The principles of fundamental justice are the shared assumptions upon which our system of justice is grounded. They find their meaning in the cases and traditions that have long detailed the basic norms for how the state deals with its citizens. Society views them as essential to the administration of justice. Third, the alleged principle must be capable of being identified with precision and applied to situations in a manner that yields predictable results. Examples of principles of fundamental justice that meet all three requirements include the need for a guilty mind and for reasonably clear laws.[389]

In *Application under s. 83.28 of the Criminal Code (Re)*,[390] the majority applied this method to determine the constitutional validity of the now-repealed anti-terrorism provision that allowed for compelled examination by the courts of witnesses. The appellant argued that s. 83.28 of the *Criminal Code* violated his right to silence and his right against self-incrimination. The Court determined that the principle against self-incrimination has constantly been interpreted as allowing the imposition of testimonial obligations on witnesses,

[389] *Canadian Foundation for Children, Youth and the Law v Canada (Attorney General)*, 2004 SCC 4, [2004] 1 SCR 76 at para 8.
[390] *Application under s. 83.28 of the Criminal Code (Re)*, *supra* note 378.

while providing protection by way of evidentiary immunity.[391] As such, s. 83.28 was deemed to not violate s. 7 of the *Charter* and the right against-self-incrimination as the disposition provided the witness with the appropriate immunities.[392]

Canadian criminal law has indeed favoured granting immunities, rather than keeping the common law right to refuse to answer questions that may incriminate oneself.[393] The crux of the matter when it comes to the application of the principle against self-incrimination to witnesses, then, is to determine the scope of the immunity required by the *Charter*. To do so, courts will need "to balance the individual's right against self-incrimination against the state's legitimate need for information about the commission of an offence,"[394] while considering the different *raisons d'être* of the principle against self-incrimination. The reliance on immunities will prove especially helpful in crafting a framework applicable to compelled decryption that respects s. 7 of the *Charter*.

B) The Rationales Behind the Principle Against Self-Incrimination

In her *Thomson Newspapers* dissent, Justice Wilson established the origins of the right against the compellability of the accused and the right against self-incrimination as being derived from the unacceptable practises that took place in England centuries ago.[395] Regardless of whether this is true or not, these practises are no longer in use today. Other rationales must then be found for the existence of the right against self-incrimination in our modern times.

---

[391] *Ibid* at para 70.
[392] See Section 4.3 *infra*.
[393] Although this has been impacted by the SCC's decision in *R v Nedelcu*, 2012 SCC 59 [2012] 3 SCR 311 [*Nedelcu*]. See Sections 4.1.2(E) and 4.2.7 *infra*.
[394] *Thomson Newspapers Ltd v Canada*, *supra* note 345 at 556.
[395] *Ibid* at 477.

According to Wigmore, twelve possible justifications exist for the continued existence of the diverse manifestation of the broad right against self-incrimination, including the protection of innocents from being declared guilty, the recognition that truthful self-incriminating answers cannot be compelled, and the promotion of an adequate balance between the state and the individual.[396] Inspired by this, as well as Ratushny's writings on the subject of self-incrimination and the Court's writings in *Dubois*, Justice Wilson concluded that the preservation of the rights against compellability and self-incrimination "is prompted by a concern that the privacy and personal autonomy and dignity of the individual be respected by the state."[397] The various rules that implicate self-incrimination are consequently validated in modern times and reflect the balance that must be achieved in the criminal justice system between the search for truth and the individual rights of the accused. Ignoring these rights could lead us to the creation of a police state.[398] Further, because some situations that implicate self-incrimination are not covered by ss. 11(c) and 13, such as the use of derivative evidence, s. 7 of the *Charter* must be interpreted as containing a residual protecting against self-incrimination.[399]

Following Justice Wilson's dissenting arguments in *Thomson Newspapers*, Justice Lamer concluded in *Jones I* that the modern-day rationale for the principle against self-incrimination is two-fold. First, it provides "protection against unreliable confessions;" and second, it provides "protection against the abuse of power by the state."[400] Justice Lamer further

[396] Wigmore, *supra* note 363, cited by Wilson J. in *Thomson Newspapers Ltd v Canada*, *supra* note 345.
[397] *Ibid* at 480.
[398] *Ibid*.
[399] While Wilson J.'s comments are made in dissent, they can be considered authoritative as they were implicitly endorsed by Lamer J. and by the majority.
[400] *Jones I*, *supra* note 343 at 250.

concluded that it is this second purpose that is at the heart of the principle against self-incrimination. Due to the adversarial nature of our criminal justice process, the state should not be allowed to conscript accused individuals into revealing their guilt.

In *British Columbia Securities Commission v Branch*, L'Heureux-Dubé J. examined the different rationales given by English courts for the protections stemming from the principle against self-incrimination.[401] According to her, the Canadian experience with self-incrimination is mostly concerned with the reliability of the compelled evidence and the possibility that it would mislead the trier of facts. This conclusion is partly aligned with what the majority concluded the same year in *R v Fitzpatrick*.[402] In this decision, the SCC examined the application of the protection against self-incrimination in the context of the *Fisheries Act* and its provisions concerning the mandatory creation and production of documents. The Court, unanimously for the first time, endorsed Lamer J.'s opinion in *Jones I* that the principle against self-incrimination is justified under the two abovementioned rationales.[403] In the case of commercial fisheries, neither of these considerations is engaged when the state seeks to use mandatorily created reports in order to prove the accused's guilt under the *Fisheries Act*.[404]

C) Delimitating the Contours of the Principle Against Self-Incrimination

In *R v S (RJ)*,[405] the SCC had the occasion to further specify the principle against self-incrimination, this time in the context of the compellability of offenders charged separately for the same offense. In a heavily split decision, a narrow majority (La Forest, Cory,

[401] *BC Securities*, *supra* note 376 at para 68.
[402] *Fitzpatrick*, *supra* note 371.
[403] *Ibid* at para 43, referring to *Jones I*, *supra* note 343 at 250.
[404] *Fitzpatrick*, *supra* note 371 at paras 43–48.
[405] *S (RJ)*, *supra* note 343.

Iacobucci, and Major JJ.) concluded that participants in a crime can indeed be compelled to testify against one another if they are charged separately. To reach this conclusion, the majority examined the principle against self-incrimination in depth, in the context of s. 7 of the *Charter*.

To determine if a principle of fundamental justice has been violated, a two-step analysis is used: "[f]irst it can be determined whether there exists a real or imminent deprivation of an interest or interests recognized in the section. Second, the relevant principles of fundamental justice can be isolated, and the deprivation can be measured against these principles to determine whether s. 7 has been infringed."[406] According to the majority, statutory compulsion to testify will necessarily implicate the liberty interest found in s. 7.[407] However, this does not necessarily mean that this compulsion is done in contravention of the principles of fundamental justice. Indeed, "the rights listed in s. 7 of the *Charter* are not guaranteed at large"[408] and they can be subject to a deprivation in accordance with the principles of fundamental justice. In this specific case, the relevant principle of fundamental justice is the principle against self-incrimination.

The Court noted that the principle against self-incrimination does not exist solely within the confines of the *Charter* but is also reflected in testimonial privileges, the confessions rule, and general policy considerations.[409] However, the *Charter* impacted the law of self-incrimination greatly. Indeed, prior to the *Charter*, the many rules that are now seen as being *derived* from the overarching principle against self-incrimination were rather construed as

---

[406] *Ibid* at para 27. See also *Jarvis I*, *supra* note 377 at para 66.
[407] *S (RJ)*, *supra* note 343 at para 42, referring to *Thomson Newspapers Ltd v Canada*, *supra* note 345.
[408] *S (RJ)*, *supra* note 343 at para 44.
[409] *Ibid* at paras 51 and following.

being the principle.[410] In the specific instance of statutorily compelled testimony, the majority concluded that the principle against self-incrimination was justified under "the principle of sovereignty embodied in the idea that individuals should be left alone in the absence of justification, and not conscripted by the state to promote a self-defeating purpose."[411] This general distaste or abhorrence for self-conscription or self-incrimination is reflected in the diverse rules that relate to self-incrimination, whether emanating from the *Charter* or not.

While there are many rules found in the *Charter* that implicate the principle against self-incrimination, it is interesting to notice that the *Charter* does not contain a "free-standing right against self-incrimination."[412] This is not surprising considering that this principle was not recognized as such prior to the advent of the *Charter* and its subsequent interpretation by the courts. Concretely, this means that the contours of the right against self-incrimination are not exclusively found in one place, but rather in the interpretation of various rules that relate to an overarching desire to prevent coerced self-incrimination, recognized as a principle of fundamental justice under s. 7 of the *Charter*.[413]

When it comes to the specific application of the principle against self-incrimination to witness compellability, as mentioned, Canada has historically favored a unique approach that makes

---

[410] *Ibid* at paras 76–77.

[411] *Ibid* at para 81. In *Application under s. 83.28 of the Criminal Code (Re)*, *supra* note 378 at para 70 the majority reiterated that the right against self-incrimination "has been recognized in relation to the principle of individual sovereignty and as an assertion of human freedom." See also *Jones I*, *supra* note 343 at 248–249; *White*, *supra* note 388 at para 43.

[412] *S (RJ)*, *supra* note 343 at para 100.

[413] See definitions of terms "coercion" and "incrimination," *infra*. See also Adelina Iftene, "Mr. Big: The Undercover Breach of the Right against Self-Incrimination" in Chris Hunt, ed., *Perspective on Evidentiary Privileges* (Toronto: Carswell, 2019) at 27, who describes "the principle against self-incrimination, descending from the much narrower privilege against self-incrimination, has [having] evolved in the Canadian jurisprudence as an overarching umbrella tying together discreet rules of evidence."

every individual compellable and forces them to answer every question, in exchange for evidentiary immunities. The *Charter* was written in a way that "attempt[s] to enact in constitutional form the same structural protection against self-incrimination for witnesses which existed historically."[414] Thus, the Canadian approach to witness compellability is a unique way of striking the balance between the individual and societal interests at play, namely to balance self-incrimination considerations with the truth-seeking function of the criminal process.[415]

However, this does not mean that individuals will be compellable in every type of procedures, even in exchange for the protection provided by evidentiary immunity. The nature of the procedures (inquisitorial as opposed to accusatorial, *vis-à-vis* the witness), as well as the purpose for which testimony is desired by the state, will need to be considered to determine if the immunity given is sufficient to mitigate the effect of the compelled testimony on the principle against self-incrimination.[416] This means that offenders charged separately can be compelled to testify at the other person's trial, but not at their own, in exchange for the relevant immunities.[417] However, a procedure that is only justified for incriminatory purposes should be forbidden.[418]

---

[414] *S (RJ)*, *supra* note 343 at para 136.
[415] *Ibid* at para 139.
[416] *Ibid* at paras 145–146. It is important to note however that the adversarial relation between the state and the individual does not need to exist at the time the compelled statement is made. The risk of being involved in such adversarial proceedings later on, based on the compelled testimony, is sufficient. See *R v Brown*, 2002 SCC 32, [2002] 2 SCR 185 at para 94 [*Brown*].
[417] See Section 4.3 *infra* for more on the different types of immunities granted to witnesses.
[418] *S (RJ)*, *supra* note 343 at para 146 *in fine*. *R v Primeau*, [1995] 2 SCR 60; *R v Jobin*, [1995] 2 SCR 78.

In *R v White*,[419] the SCC examined if statements regarding accidents made under compulsion under the *Motor Vehicle Act* of British-Columbia were admissible during a criminal trial, under the principle against self-incrimination. In order to do so, Iacobucci J. applied the four following factors that are adapted from *Fitzpatrick*: (1) existence (or lack) of coercion; (2) presence (or absence) of an adversarial relationship between the accused and the state; (3) presence (or absence) of an increased risk of unreliable confession as a result of the statutory compulsion; and (4) presence (or absence) of an increased risk of abuses of power by the state as a result of the statutory compulsion.[420]

To determine if coercion existed in the context of the obligation to disclose accidents found in the *Motor Vehicle Act*, the Court adopted a highly fact-dependent circumstantial approach that considers the place that driving takes in modern life, as a regulated and voluntary activity. As it will be further explained *infra*,[421] the Court eventually found that this factor was neutral in this case.

On the second factor, the decision of the province to make police officers responsible for taking accident reports was found to be determinative, as it has the potential to transform the relationship between the individual and the state into one of adversarial nature. The police officer receiving the mandatory accident report is often simultaneously investigating a possible crime and may even sometimes feel the need to disclose that information, as well as inform the driver about their legal rights, including the right to remain silent. For this reason, it cannot be said that the relationship at that point between the driver and the police officer is

[419] *White*, *supra* note 388.
[420] *Ibid* at para 51.
[421] See Section 4.1.2 (D), *infra*.

neutral or collaborative.[422] This potential adversarial relationship between drivers and law enforcement officers raises important concerns about the possibility of unreliable confessions, the third factor of the *Fitzpatrick* analysis, and about possible abusive conduct by the state, which is the fourth factor. Drivers may feel the need to lie about their involvement in an accident when they are interacting with a person in authority, while police officers may try to further their investigation by using the mandatory disclosure obligations, even when they are in fact investigating a criminal offense.[423]

In the end, the SCC found that the principle against self-incrimination did not protect drivers from having to make the statement under the provincial statute but protected them from its subsequent use to incriminate them during a criminal trial. According to the Court, the creation of this immunity against the use of mandatory accident reports in the course of a criminal investigation "is itself a balancing between society's goal of discovering the truth, on the one hand, and the fundamental importance for the individual of not being compelled to self-incriminate, on the other."[424] In that sense, it does not put the principle against self-incrimination above other principles of fundamental justice, but only balances the different principles at play. To reach this conclusion, the majority also examined and summarized the previous SCC decisions on self-incrimination, ranging from *Thomson Newspapers* to *Fitzpatrick*. Recognizing that the principle against self-incrimination is the source of numerous well-known rules within the Canadian justice system, the majority opened the door

[422] *White*, *supra* note 388 at para 58.
[423] *Ibid* at paras 61–66.
[424] *Ibid* at para 71.

to the fact that "the principle can also be the source of new rules in appropriate circumstances,"[425] such as is being discussed here.

The majority in *Hart*[426] also created a new rule related to self-incrimination, although it decided to do so without applying the framework established in *White*. In this decision, the Court had to examine the admissibility of the "Mr. Big technique," which is a Canadian creation used when law enforcement comes to a dead end in a criminal investigation. Such operation is described in the decision in the following manner:

> A Mr. Big operation begins with undercover officers luring their suspect into a fictitious criminal organization of their own making. Over the next several weeks or months, the suspect is befriended by the undercover officers. He is shown that working with the organization provides a pathway to financial rewards and close friendships. There is only one catch. The crime boss — known colloquially as "Mr. Big" — must approve the suspect's membership in the criminal organization.[427]

The majority stated that Mr. Big operations definitely raise concerns related to the principle.[428] However, it decided that resolving this issue did not require using the *White* framework, as creating a two-pronged approach under a common law evidentiary rule and the doctrine of abuse of power was better in this specific case. In doing so, the Court nonetheless recognized that this two-pronged approach addresses the same considerations as the principle against self-incrimination, as they both seek to protect individuals against abusive state conduct and guards the criminal justice system against unreliable statements by accused persons. For this reason, the majority's avoidance of solving this issue using the *White* framework seems more

[425] *Ibid* at para 44.
[426] *Hart*, *supra* note 379.
[427] *Ibid* at para 1.
[428] *Ibid* at paras 123–125.

like a question of choice than an actual disagreement over the substance of the protection provided by the principle against self-incrimination.[429]

The SCC mostly analyzed the principle against self-incrimination in the context of verbal declarations, not "real" evidence. However, *R v SAB* opened to door to the application of the principle to material evidence. In 2003, the SCC in *SAB*[430] specified the interaction between ss. 7 and 8 when it considered whether the privilege against self-incrimination is triggered when it comes to the execution of DNA warrants for investigative purposes. Justice Arbour, writing for a unanimous Court, started her analysis by stating that the principle against self-incrimination was better considered under s. 8 of the *Charter* in this case, rather than under s. 7, because of the nature of the state conduct, which can be qualified as a search or a seizure. The Court thus stated that "real" evidence, as opposed to oral testimony, can also implicate the principle against self-incrimination—albeit in a different manner—and that search and seizure law does not solely implicate privacy interests but also other considerations such as self-incrimination.[431]

---

[429] In dissent, Karakatsanis J. based her analysis of the Mr. Big technique on the principle against self-incrimination. She found that "[t]he very structure of such operations creates circumstances that (1) compromise the suspect's autonomy; (2) undermine the reliability of the confession; and (3) raise concern about abusive state conduct," all of which are related to the principle against self-incrimination. She also stressed the fact that Mr. Big operations directly involve the inequity of resources that exists between the state and the individual when it comes to criminal law, and that using the principle against self-incrimination in this context avoided the creation of a new rule, as the scope of the protection required by s. 7 is to be determined on a case-by-case basis according to *Jones I*. She would have applied the *White* framework to determine that the result of the Mr. Big operation was inadmissible. *Ibid* at paras 164–243. For a criticism of the majority's decision, see also Iftene, *supra* note 413.

[430] *R v SAB*, 2003 SCC 60, [2003] 2 SCR 678 [*SAB*].

[431] *Ibid* at paras 33–35, referring to *Stillman*, *supra* note 353 at paras 83–86; *Hunter*, *supra* note 31 at 159; *R v Mills*, [1999] 3 SCR 668 at para 88 [*Mills I*].

To some extent, *Stillman* also addressed the possibility of applying self-incrimination considerations to material evidence, if only under s. 24(2) of the *Charter*. The majority mentioned that compelled use of bodily substances or characteristics can also implicate self-incrimination interests, even if the material evidence exists absent of the compulsion.[432] The Court concluded that "[t]he compulsion which results in self-incrimination by a statement or the taking of bodily substances or the use of the body itself may arise in a number of ways such as the forced participation in a line-up identification; providing a breath sample; providing DNA samples – blood, telling the police where to find evidence; and making an incriminating statement."[433] Thus, the principle against self-incrimination can be applied to situations where material evidence is the object of the compulsion, not just testimonial evidence.

That being said, *Stillman* has been overturned in *R v Grant*, *inter alia* because it created an automatic exclusion regime for conscriptive evidence, which does not respect the wording of s. 24(2) of the *Charter*.[434] Following *Grant*, material conscriptive evidence is not to be automatically excluded under s. 24(2), but rather the totality of the circumstances must be examined to determine if the exclusion is necessary to avoid bringing the administration of justice into disrepute.[435] Even so, *Grant* did not overturn the general conclusion that the principle against self-incrimination can be applied to real evidence, following *Stillman*. In essence, self-incrimination considerations are engaged when an individual does not have a

[432] *Stillman*, *supra* note 353 at paras 80–91.
[433] *Ibid* at para 94 (references omitted).
[434] *R v Grant*, 2009 SCC 32, [2009] 2 SCR 353 [*Grant*]. For a critique of the *Stillman/Collins* framework, see *R v Côté*, 2011 SCC 46, [2011] 3 SCR 215 at para 65.
[435] *Grant*, *ibid* at 105.

choice but to collaborate with the authorities.[436] As such, testimonial and non-testimonial evidence can raise self-incrimination considerations, if the choice to engage with the authorities is removed. However, the degree of protection given to testimonial and non-testimonial self-incrimination differs.

Testimonial self-incrimination is usually protected with more vigor, by way of the right to remain silent which is nearly absolute in Canada.[437] In contrast, non-testimonial self-incrimination is protected to a lesser degree and with more flexibility. As explained by Lee Stuesser, there is indeed a distinction to be made between testimonial and non-testimonial self-incrimination in Canada.[438] Testimonial and non-testimonial (or real) evidence do not raise exactly the same considerations when it comes to self-incrimination, *inter alia* because non-testimonial physical evidence is inherently reliable.[439] *SAB*, by confirming the constitutional validity of coerced DNA sampling under both ss. 7 and 8, "reinforces the different approach to "testimonial" versus "non-testimonial" self-incrimination,"[440] without however closing the door completely to the application of the principle against self-incrimination to non-testimonial evidence. As explained by Stuesser:

> Simply put, "testimonial" self-incrimination is guarded more rigorously by the courts then "non-testimonial" conscription. In "testimonial" cases such as *R v Hebert*, a right to silence case, and *R v White*, where compelled statements were used against the

[436] See Section 4.1.2 (D) *infra*.
[437] See Sections 4.2.1 and 7.3.1(A), *infra*.
[438] Lee Stuesser, "*R v S.A.B.*: Putting "Self-Incrimination" in Context" (2004) 42:2 Alta L Rev 543 at 548. This is accepted by many authors. See *inter alia* David M Paciocco, "Self-Incrimination: Removing the Coffin Nails" (1990) 35 McGill LJ 73; Penney & Gibbs, *supra* note 3 at 231 (who further decline non-testimonial evidence as regrouping linguistic and non-linguistic evidence).
[439] *Ibid* at 548, citing McLachlin's J. dissenting reasons in *Stillman*, *supra* note 353 at 202. This was also accepted by the majority in *SAB*, *supra* note 430 at para 58.
[440] *Ibid* at 549.

> person, the principle against self-incrimination was invoked to fashion a *Charter* right. In contrast, the courts have in "non-testimonial" cases upheld the taking of fingerprints from suspects, roadside breath demands, and now the taking of DNA samples.[441]

The contrast in treatment between testimonial self-incrimination and non-testimonial self-incrimination can also be seen in *R v Orbanski; R v Elias*,[442] where the SCC examined the constitutional validity of roadside sobriety tests. In this decision, the majority concluded that the self-incriminating aspects of sobriety testing were sufficiently addressed by the limited use that can be made of that evidence during the screening process and subsequently at trial to establish guilt.[443] This demonstrates that some incriminating evidence can sometimes be compelled, especially when it is non-testimonial in nature, and that the impact of that compulsion on the right against self-incrimination will be alleviated by evidentiary and procedural rules.

This distinction between the application of the principle against self-incrimination to testimonial and non-testimonial evidence will become important later on in this thesis to determine whether or not compelled decryption can be allowed under s. 7 of the *Charter*. Compelled decryption—unlike other investigative techniques—is on the cusp of both types of evidence: the coerced act of decryption is *testimonial*,[444] while the data it gives access to is pre-existing *non-testimonial* evidence. *A contrario*, "traditional" compelled statements are purely testimonial: the prosecution is seeking their admission into evidence to prove the truth of their content. This conclusion will allow for the recognition that compelled decryption is

---

[441] *Ibid* at 549-550.
[442] *R v Orbanski; R v Elia*, 2005 SCC 37, [2005] 2 SCR 3 [*Orbanski*].
[443] *Ibid* at para 58-59.
[444] It is a statement of the ability to decrypt, which will usually also imply control or ownership over the data or device. See Section 7.2.1(B) *infra*.

acceptable under s. 7 of the *Charter*, when strict requirements are imposed on law enforcement and when the accused is granted immunity towards the testimonial self-incriminating aspects of the act of decryption.[445]

As a final note to this section, it is worth restating that the principles of fundamental justice are not concerned solely with accused individuals but also with more global societal interests. As such, the principle against self-incrimination, even as a core principle of fundamental justice, does not give the accused the right to "the most favourable procedures that could possibly be imagined."[446] It gives the accused the right to fair procedures, not procedures that consider only their individual or personal interests. The right against self-incrimination, then, as a principle of fundamental justice, seeks to balance opposed interests at play by creating protections that are *reasonable*, when considering individual rights and social interests.[447]

D) The Definition of "Coercion"

As mentioned previously, in *Jones I* Lamer J., defined coercion (or compulsion) as the absence of free and informed consent.[448] In other words, coercion is the absence of choice, which can be linked to the principle of sovereignty of the individual. This is also consistent

[445] See generally Chapter 7 *infra*.
[446] *Lyons*, *supra* note 383 at 362, cited in *Darrach*, *supra* note 388 at para 24 and *Mills I*, *supra* note 431 at para 72. See also *R v JJ*, 2022 CSC 28, at para 125 and *Seaboyer*, *supra* note 388, at 611 (as per McLachlin J., writing for the majority) and 692 (as per L'Heureux-Dubé J., in dissent), where the SCC reaffirmed the fact that a judge can exclude evidence presented by the defence, if its prejudicial effect substantially outweighs its value.
[447] See also Section 7.1.2 *infra*.
[448] *Jones I*, *supra* note 343 at 249. See also *White*, *supra* note 388 at para 42; *Darrach*, *supra* note 388 at para 49.

with the majority's decision in *Hebert*, where self-incrimination was linked to the right *to choose* to collaborate or engage with the authorities.[449]

In *Fitzpatrick*, the SCC reiterated that the protection against self-incrimination that emanates from s. 7 is not a broad and abstract principle that forbids compulsion in every situation and that the context will dictate the scope of the protection.[450] In the specific case of commercial fisheries, a regulated activity, the principle against self-incrimination does not dictate that the accused be granted immunity against the use of his statutorily compelled reports. The SCC concluded that individuals are not in an adversarial relationship with the state when they create fishing logs and disclose them to the state, and that there is a lack of coercion in the relationship between the state and the individual, mostly due to the fact that individuals who engage in fishing do so voluntarily.[451] The fact that the information compiled by individuals involved in commercial fishery may later be used against them by the state when it seeks to enforce the applicable regulations does not change this conclusion.[452] Thus, the fact that the accused had *chosen* to participate in commercial fisheries weighed heavily in the Court's decision in *Fitzpatrick.*

In *White*, the Court considered the prosecution's argument that driving, as a regulated activity, entails that drivers agree to the rules of the road, including the obligation to report accidents under the *Motor Vehicle Act.* The prosecution also stressed the fact that driving had previously been qualified as voluntary by the SCC.[453] However, the Court determined that "[w]hen a

[449] *Hebert*, *supra* note 384 at 174-177. See also Iftene, *supra* note 413 at 27.
[450] *Fitzpatrick*, *supra* note 371 at paras 21–24, 29–32.
[451] *Ibid* at paras 33–39.
[452] *Ibid* at para 42.
[453] *Dedman v The Queen*, [1985] 2 SCR 2 [*Dedman*]; *R v Hundal*, [1993] 1 SCR 867; *R v Finlay*, [1993] 3 SCR 103.

person needs to drive in order to function meaningfully in society, the choice of whether to drive is not truly as free as the choice of whether to enter into an industry."[454] Qualifying the obligation to disclose accidents under the *Motor Vehicle Act* as being coercive is difficult in a context where individuals voluntarily decide to participate in an activity such as driving, but we must also bear in mind that human freedom lies at the center of the principle against self-incrimination and that this freedom is somewhat impacted by the abovementioned obligation. After considering the other factors described in *Fitzpatrick*, the Court concluded "that a statement made under compulsion of s. 61 of the *Motor Vehicle Act* cannot be used to incriminate the declarant in subsequent criminal proceedings."[455]

To determine if indeed coercion is present in a specific case, the Court determined that the subjective beliefs of the individual must be examined, as "compulsion, by definition, implies an absence of consent."[456] This subjective belief must also be objectively reasonable, otherwise there is no risk of true oppression by the state, which is what the principle against self-incrimination seeks to avoid.[457] As such, "[t]he requirement that an honest belief be reasonably held is an essential component of the balancing that occurs under s. 7. The application of the principle against self-incrimination begins, and the societal interest in the effective investigation and prosecution of crime is subordinated, at the moment when a driver speaks on the basis of a reasonable and honest belief that he or she is required by law to do so."[458]

---

[454] *White*, *supra* note 388 at para 55.
[455] *Ibid* at para 67.
[456] *White*, *supra* note 388 at para 76.
[457] *Ibid* at para 77.
[458] *Ibid*.

The SCC also examined the definition of coercion in *Henry*,[459] where the two appellants told a different story at their retrial than they had previously at the first trial. The appellants argued that s. 13 of the *Charter* protected them against such use of their previous statements to incriminate them during their cross-examination. Distinguishing this situation from the one which prevailed in *Dubois* where the accused did not testify at his retrial, the Court determined that the fact that the accused had *chosen* to testify at their retrial means that there is no coercion and that the privilege against self-incrimination was not engaged.[460] Choice, then, is at the heart of the principle against self-incrimination, which arguably provides a third rationale to the principle: individual autonomy and personal sovereignty.[461]

E) The Definition of "Incrimination"

The SCC struggled for a long time to establish when the use of a prior testimony was indeed used to "incriminate," as opposed to being used to impeach the accused's credibility.[462] In *Henry*, the SCC unanimously determined that this distinction was difficult to apply in practice and that it was unrealistic in the context of s. 5(2) of the *Canada Evidence Act* and of s. 13 of the *Charter*. Accordingly, the SCC concluded that the use of a prior compelled testimony is,

[459] *Henry*, *supra* note 354.
[460] *Henry*, *supra* note 354 at para 47. This effectively overturned *R v Mannion*, [1986] 2 SCR 272 [*Mannion*] and some parts of *Kuldip*, *supra* note 357.
[461] As stated by Iftene, *supra* note 413 at 28, a third rationale to the principle against self-incrimination is often referred to by scholars, namely that self-incrimination is also justified by a desire to "[uphold] individual autonomy, sovereignty, dignity, and privacy interests." The link between self-incrimination and privacy will become especially relevant when it comes to compelled decryption, as the self-incriminating act of decryption will give law enforcement access to private information. See Chapter 7 *infra*.
[462] The SCC recognized the existence of this struggle *inter alia* in *R v Noël*, 2002 SCC 67 [2002] 3 SCR 433 at para 20, 27; *Kuldip*, *supra* note 357 at 635 and *Henry*, *supra* note 354 at paras 35, 45.

under both provisions, inadmissible, regardless of the reason why the prosecution is seeking its admissibility.[463]

In 2012, the SCC revisited this distinction and examined the notion of incrimination in *R v Nedelcu*.[464] Justice Moldaver, writing for the majority, stated that evidence will be qualified as incriminating if it is used "to prove guilt, i.e., to prove or assist in proving one or more of the essential elements of the offence for which the witness is being tried."[465] To be qualified as such, the nature of the evidence will need to be examined at the moment the Crown is seeking to use it at the subsequent proceedings.[466] Specifically in this case, the majority concluded that the accused's prior compelled testimony was not incriminating, as it could not be used by the prosecution "to prove or assist in proving one or more of the essential elements of the criminal charges [the accused] was facing,"[467] as the prior statement made by the accused was that he did not remember anything from the night of the alleged crime.

Moldaver J. went on to determine that the protection given by s. 13 of the *Charter* is based on the presence of a *quid pro quo*, where the *quid* refers to incriminating evidence and the *quo* to the immunity given to the use of that evidence to incriminate the witness in another procedure.[468] For that reason, when the evidence is not incriminating (as defined *supra*), the protection of s. 13 is not engaged, nor is the general principle against self-incrimination. In

---

[463] *Henry*, *supra* note 354 at paras 50-51.
[464] *Nedelcu*, *supra* note 393.
[465] *Ibid* at para 9.
[466] *Nedelcu*, *supra* note 393 at para 16. This accounts for the fact that evidence that is "seemingly innocuous or exculpatory at the time [of the first proceeding], may become "incriminating evidence at the subsequent proceeding." *Ibid* at para 17. However, as stated by Lisa Dufraimont, "[t]he new "incriminating evidence" requirement introduced in *Nedelcu* focuses not on the *use* of the evidence, but on its *nature*." See Lisa Dufraimont, "Section 13 Immunity After *R v Nedelcu*" (2012) 96 CR (6th) 431 at 2.
[467] *Nedelcu*, *supra* note 393 at para 20.
[468] *Ibid* at paras 3–7.

other words, even if testimony or the production of evidence is compelled, its use will not engage the protection against self-incrimination if it cannot be qualified as being *incriminating* in the first place. While this conclusion has not officially reversed *Henry* when it comes to the inadmissibility of compelled incriminating evidence (either to impeach credibility or to prove guilt),[469] it has dramatically reduced the scope of the protection offered by s. 13 of the *Charter*, by redefining what constitutes *incrimination* in such a narrow way.[470] This seems difficult—if not impossible—to reconcile with the definitions given to this term in *Jones I*, where Lamer J. specified that the word "incriminate" in the context of the principle against self-incrimination does not equate with "tending to prove guilt of a criminal offence."[471]

The dissenting judges (LeBel, Fish, and Cromwell JJ.) were cognizant of the negative impact of the majority's decision on the breadth of the principle against self-incrimination. Applying the *ratio decidendi* from *Henry*, the dissenting judges concluded that the prior statement made by the accused was inadmissible, as it had been made under compulsion and it was being used to impeach the accused's credibility.[472] As they did not see any valid reason to reconsider *Henry*,[473] they concluded that the majority's position was inconsistent with the judicial precedents.[474] They also stressed the fact that the truth-seeking function of the criminal trial

[469] Indeed, Moldaver J. specifically mentioned that if the previous testimony can be qualified as incriminating under this new definition of the term, the prosecution will not be allowed to use to impeach the accused's credibility. See *Ibid* at para 15. See also Dufraimont, *supra* note 466 at 2.
[470] Walker, *supra* note 354 at para 49.
[471] *Jones I*, *supra* note 343 at 250
[472] *Ibid* at para 95 [as per Lebel J.'s dissenting reasons].
[473] *Ibid* at paras 115-116.
[474] *Ibid* at para 129.

must sometimes yield way to other considerations, such as protecting individuals from coerced self-incrimination.[475]

4.2 The Different Protections Related to the Principle Against Self-Incrimination

As mentioned previously, Lamer J. in *Jones I* listed a series of rules, rights, and privileges that emanate from the principle against self-incrimination.[476] These different rules create a comprehensive system that aim to protect individuals against compelled self-incrimination, whether during the pre-trial or the trial phases of the criminal process.

Not all these rules will be relevant when it comes to compelled decryption. Accordingly, only the ones relevant to the overarching goal of this thesis will be analyzed, principally the right to silence and the right to counsel. It is worth stating up front that use and derivative use immunity, two trial phase protections against self-incrimination, are analyzed here to demonstrate that immunities can be used to alleviate the impacts of coerced self-incrimination on individual rights. The following section is an overview of how these specific protections take root in (or interact with) the principle against self-incrimination. It is not a detailed or thorough analysis of the jurisprudence on each single protection and all their various and specific applications.

[475] *Ibid* at paras 119-120. See Section 4.2.7 *infra* for the criticism of the majority's decision in *Nedelcu*.
[476] *Jones I*, *supra* note 343 at 252–255.

4.2.1 The Right to Silence

As mentioned previously, the right to remain silent was not always seen as emanating from a general principle against self-incrimination. However, after the advent of the *Charter*, the right to silence became more than a proxy for the idea that individuals do not have an obligation to help or assist law enforcement.

In *Hebert*, McLachlin stated that "the measure of the right to silence may be postulated to reside in the notion that a person whose liberty is placed in jeopardy by the criminal process cannot be required to give evidence against himself or herself, but rather has the right to choose whether to speak or to remain silent."[477] The right to silence is inextricably linked to the principle against self-incrimination because that is effectively what it aims to prevent: the involuntary utterance of self-incriminating declarations. In other words, the right to silence is "the right not to incriminate oneself with one's words."[478] In that sense, without free and informed consent to speak to the authorities, the right to silence is infringed.[479] The right to silence thus comes into play every time a person interacts with the authorities, whether detained or not; "[it] is a right premised on an individual's freedom to choose the extent of his or her cooperation with the police, and is animated by a recognition of the potentially coercive impact of the state's authority and a concern that individuals not be required to

[477] *Hebert*, *supra* note 384 at 175.
[478] *Ibid* at 195 per Sopinka J. (concurring).
[479] *Jones I*, *supra* note 343 at 253. This is also a concern of the common law confessions rule, which is not examined here.

incriminate themselves."[480] The right to pre-trial silence, however, does not include the right not to be spoken to by the authorities.[481]

The majority in *Noble* also considered the link between the right to silence and the principle against self-incrimination. As per Sopinka J.'s reasons:

> The accused's non-compellability at trial is now constitutionally protected under s. 11(c), but there has also been recognition of a right to silence as a principle of fundamental justice in s. 7. *R c Hebert*, [1990] 2 SCR 151, established that there is a right to silence under the *Charter* which is engaged when a person is subject to the coercive power of the state. This occurs upon arrest, charge or detention of the individual. It is at this point that an adversarial relationship is created between the state and the individual.[482]

While this statement concerns the right to silence in pre-trial procedures, the Court in *Noble* mostly considered the inferences that can be drawn from a failure of the accused to testify at trial. The Court considered that "[t]he right to silence is based on society's distaste for compelling a person to incriminate him-or her-self with his or her own words."[483] As such, the Court concluded that the trier of facts cannot consider the silence of the accused as a means of proving guilt beyond a reasonable doubt, as the pre-trial right to silence and the principle against self-incrimination would be severely undercut by doing so.[484]

Further, the presumption of innocence would also be affected by such use of the accused's silence, as it would effectively displace some of the burden of establishing guilt onto the

---

[480] *R v Turcotte*, 2005 SCC 50, [2005] 2 SCR 519 at para 51.
[481] *R v Singh*, [2007] 3 SCR 405 at para 28 [*Singh*].
[482] *R v Noble*, [1997] 1 SCR 874 at para 70 [*Noble*].
[483] *Ibid* at para 75.
[484] *Ibid*.

accused.[485] However, this does not mean that the silence of the accused at trial will not have any consequences, as once a case to meet has been established by the prosecution, accused individuals risk being declared guilty if they decide not to respond to evidence.[486]

It should also be emphasized that the right to silence does not apply to witnesses at the trial stage of proceedings, including to the accused who chooses to testify. Witnesses do not benefit from the right to remain silent at trial and instead receive a protection by way of privilege.[487]

4.2.2 The Right to Counsel

> *Everyone has the right on arrest or detention … to retain and instruct counsel without delay and to be informed of that right.*[488]

The right to counsel gives detained individuals the means to be aware of their right against self-incrimination, by informing them that they do not have to make any declaration to the police. The power to enforce that right stems from the right to silence. As such, "[t]he purpose of s. 10(b) … is the fostering of the right against self-incrimination."[489] In other words:

> The right to counsel is primarily aimed at preventing the accused or detained person from incriminating herself. Thus the main concern would be with coerced or uninformed confessions. In such circumstances, the accused would be manufacturing

[485] *Ibid* at para 76.
[486] *Darrach*, *supra* note 388 at para 54.
[487] See *infra*.
[488] *Charter*, *supra* note 24, s 10(b).
[489] *Jones I*, *supra* note 343 at 255. See also *R v Suter*, 2018 SCC 34, [2018] 2 SCR 496 at para 177; *Singh*, *supra* note 481 at para 21.

> the evidence against herself. This is something which, in the interests of fairness, the right to counsel would seek to protect.[490]

The right to counsel is triggered when an individual is detained by law enforcement, as it puts them in a vulnerable position towards the state. As such, the right to counsel seeks to re-equilibrate the power between the detained individual and the state, by giving the former the means to know that they have a choice to speak to the latter.[491] Because of the importance of the right to counsel in relation with other rights, namely the right to silence and the right against self-incrimination, violation of the right to counsel will tend to militate towards the exclusion of the obtained statements, under s. 24(2) of the *Charter*, unless particular circumstances attenuate the impact of the breach.[492]

Further, detained individuals need to understand the extent of their jeopardy, "that is, the nature and extent of [their] risk of self-incrimination,"[493] in order to make a free and informed choice to collaborate with the authorities or to remain silent. This means law enforcement needs to give detained individuals their right to counsel "without delay," or immediately in this context,[494] and they might need to restate the right to counsel if the circumstances of the investigation change.[495] This immediate right to counsel "is meant to assist detainees regain their liberty, and guard against the risk of involuntary self-incrimination."[496]

---

[490] *R v Simmons*, [1988] 2 SCR 495 at 539 [*Simmons*], cited in *Jones I*, *supra* note 343 at 255. See also *S (RJ)*, *supra* note 343 at para 85, where Iacobucci J. endorsed Lamer's comments on the link between self-incrimination and the right to counsel from *Jones I*.
[491] *Grant*, *supra* note 434 at para 22.
[492] *Ibid* at paras 95–96.
[493] *R v Sawatsky*, [1997] CanLII 511 (ON CA) at 15.
[494] *R v Suberu*, 2009 SCC 33, [2009] 2 SCR 460 at paras 40–42 [*Suberu*].
[495] *R v Evans*, [1991] 1 SCR 869 at 306–307.
[496] *Suberu*, *supra* note 494 at para 40.

To be clear, the right to counsel does not remove the possibility of self-incrimination: a detained individual might decide to make a declaration to the authorities after having consulted with a lawyer or after refusing to contact one. The authorities are also allowed to continue asking questions of a detained individual or to generally try to elicit evidence from them, after the detainee has consulted with a lawyer if they desire to do so, or if they do not indicate a desire to speak with counsel.[497] Section 10(b) of the *Charter* is then linked to self-incrimination in the limited sense that it requires law enforcement to inform individuals of their right against involuntary self-incrimination.

4.2.3 The Privilege Against Self-Incrimination and its Related Use Immunity

> *A witness who testifies in any proceedings has the right not to have any incriminating evidence so given used to incriminate that witness in any other proceedings, except in a prosecution for perjury or for giving of contradictory evidence.*[498]

Prior to the adoption of s. 5 of the *Canada Evidence Act* and of s. 13 of the *Charter*, the privilege against self-incrimination allowed witnesses to refuse to answer questions that could tend to incriminate them. In *R v Noël*, Arbour J. summarized the common law privilege against self-incrimination as follows:

> The common law "privilege" against self-incrimination, traditionally expressed in the maxim *nemo tenetur seipsum accusare,* is a particular rule derived from the broader "principle" against self-incrimination: *R. v. Jones*, [1994] 2 S.C.R. 229. At common law, the accused was neither competent nor compellable as a witness. For the non-accused witness however, the common law privilege against self-incrimination

[497] The obligation of refraining to elicit evidence from the detained individual is only applicable until they have had a reasonable opportunity to exercise their right to counsel. See *inter alia R v Taylor*, 2014 SCC 50, [2014] 2 SCR 495, at 23; *Singh*, *supra* note 481 at para 47.
[498] *Charter*, *supra* note 24, s 13.

> provided that everyone was entitled to refuse to answer a question which might incriminate him: *R. v. Marcoux*, [1976] 1 S.C.R. 763. As such, the rule was aptly called the "privilege" against self-incrimination or the "prerogative" of the witness. See *R. v. Tass* (1946), 86 C.C.C. 97 (Man. C.A.), at pp. 104-5, for a convenient summary of the common law privilege against self-incrimination. That privilege is thus distinct from the concept of compellability. Save for a few — the accused and his or her spouse — all witnesses are compellable to give evidence. Whether they do so enthusiastically, voluntarily, reluctantly or under the threat of legal sanction, witnesses are required to appear, to take an oath and to answer truthfully all questions put to them, subject to the common law privilege or, now that it has been modified by statute, to the protection offered by s. 5 of the *Canada Evidence Act*.[499]

By imposing an obligation to all witnesses to answer any questions asked before them even if the answer could incriminate them, s. 5(1) of the *Canada Evidence Act* abolished the common law privilege against self-incrimination in Canada.[500] To counterbalance that obligation, s. 5(2) provides immunity to that witness for the subsequent use of their incriminating testimony, except in the case of prosecution for perjury related to that testimony. The decision to let go of the traditional common law rule that allows witnesses to refuse to answer questions on the basis of potential self-incrimination in favor of use immunity has been interpreted as a demonstration of the value the Canadian criminal justice system places on the search for the truth of a case.[501]

To benefit from the protection under s. 5 of the *Canada Evidence Act*, the witness has to object before answering the question. However, with the adoption of s. 13 of the *Charter*, the Canadian version of the privilege against self-incrimination was granted automatically to

[499] *Noël*, *supra* note 459 at para 35.
[500] *Thomson Newspapers Ltd v Canada*, *supra* note 345 at 474.
[501] Walker, *supra* note 354.

witnesses, without the need to previously object, effectively extending the protection that had historically been provided only by s. 5 of the *Canada Evidence Act*,[502] and addressing criticism that had been raised towards s. 5(2).[503] Both these provisions contain a very specific form of protection against self-incrimination, which is testimonial self-incrimination at trial. As such, they are complementary to the protection against self-incrimination found in other specific rules and more generally under the overarching principle against self-incrimination found in s. 7 of the *Charter*.[504]

The purpose of s. 13 of the *Charter* has been described as "[the protection of] individuals from being indirectly compelled to incriminate themselves, to ensure that the Crown will not be able to do indirectly that which s. 11(c) prohibits."[505] Both the statutory and the constitutional versions of the privilege work on the basis of a *quid pro quo*: "when a witness who is compelled to give evidence in a court proceeding is exposed to the risk of self-incrimination, the state offers protection against the subsequent use of that evidence against the witness in exchange for his or her full and frank testimony."[506] This means that the accused who voluntarily decides to testify in his defence at a retrial cannot claim the protection of s. 13 because there is absence of the compulsion aspect of the *quid pro quo* that makes the immunity found in s. 13 applicable.[507] However, when the accused does not wish to testify at a retrial, the protection of s. 13 prohibits the prosecution to adduce into evidence the testimony

[502] *Henry*, *supra* note 354 at para 23.
[503] *S (RJ)*, *supra* note 343 at para 115.
[504] Prior to *Thomson Newspapers*, it was however generally accepted that ss. 11(c) and 13 of the *Charter* constituted the entire protection against self-incrimination. See *Jones I*, *supra* note 343 at 256.
[505] *Dubois*, *supra* note 360 at 358.
[506] *Noël*, *supra* note 459 at para 21, cited in *Henry*, *supra* note 354 at para 22.
[507] *Henry*, *supra* note 354.

of the accused given at the previous trial, as it would effectively amount to compelling that person to testify against themselves at the retrial, indirectly doing what s. 11(c) prohibits.[508]

As mentioned previously, the incriminating aspect of the *quid pro quo* that engages s. 13 of the *Charter* was examined by the SCC in *R v Nedelcu*. In this case, the prosecution was seeking to use the accused's testimony during his examination in the related civil action during his criminal trial. The SCC decided that s. 13 of the *Charter* did not prohibit such use of the prior testimony because the testimony itself was not incriminating in nature, as it could not be used to prove guilt.[509] Since this decision, an individual claiming the protection of s. 13 of the *Charter* will need to prove "premièrement que le témoignage en question a été contraint; et, deuxièmement, que ce témoignage est incriminant."[510]

It is worth mentioning that *Nedelcu* has not been well received by commentators, including on the basis that it brings back an "unworkable distinction" between using a statement to impeach credibility as opposed to using it to prove guilt.[511] The majority's decision has also been criticized because it fails to recognize that it effectively overturned *Henry*, while claiming to follow it.[512] *Nedelcu* has also been described as providing a "contrived and unstable" definition of incrimination,[513] and to have unduly narrowed the scope of the right

[508] *Dubois*, *supra* note 360.
[509] *Nedelcu*, *supra* note 393.
[510] *R c Lauzon*, 2019 ONCA 546 at para 6. See also Dufraimont, *supra* note 466 at 1.
[511] Sara Hanson, "*R v Nedelcu*: The Right Against Self-Incrimination and the Return to the Unworkable Distinction" (24 November 2012), online: *The Court* <http://www.thecourt.ca/r-v-nedelcu-the-right-against-self-incrimination-and-the-return-to-the-unworkable-distinction/>.
[512] *Ibid*.
[513] Don Stuart, "Vagueness, Inconsistency and Less Respect for Charter Rights of Accused at the Supreme Court in 2012-2013" (2013) 63 SCLR: Osgoode's Annual Constitutional Cases Conference 441 at 456.

against testimonial self-incrimination.[514] Further, while s. 13 of the *Charter* was originally conceived as expanding the protection against testimonial self-incrimination found in s. 5(2) of the *Canada Evidence Act*,[515] there seems to be a movement towards using this latter provision, to address the perceived problems caused by *Nedelcu*.[516]

How is it possible then to reconcile *Nedelcu* with the rest of the SCC's jurisprudence on self-incrimination? The only possible way to do this is possibly to focus on the specific facts of that case. In *Nedelcu*, the accused had affirmed having no recollection of the alleged crime during his prior testimony, while he gave a detailed account of the facts during his subsequent criminal trial. As Dufraimont notes, even under the modified threshold for what can be qualified as incriminating evidence, the decisions discussed in *Henry* (namely *Dubois*, *Mannion*, *Kuldip*, *Noël* and *Allen*) would not have yielded a different result, as the evidence in those cases was clearly incriminating, even under the *Nedelcu* analysis.[517] Conceived in this manner, *Nedelcu* could possibly be nothing more than a highly circumstantial application of s. 13 of the *Charter*. In any case, it will become clear in Chapter 7 that compelled decryption implicates incrimination, even under the more limited interpretation of that term emanating from *Nedelcu*.

4.2.4 Derivative Use Immunity under s. 7 of the Charter

Under s. 5 of the *Canada Evidence Act* and s. 13 of the *Charter*, compellable witnesses—whether actually compelled to testify or voluntarily doing so—must answer all questions

---

[514] Paul Calarco, "*R v Nedelcu*: Whatever Happened to a Large and Liberal Interpretation of *Charter* Rights?" (2012) 96 CR (6th) 438.
[515] *Henry*, *supra* note 354 at para 23.
[516] Stuart, *supra* note 513 at 457.
[517] Dufraimont, *supra* note 466 at 3.

asked by the prosecution and the defense, even the ones that could tend to incriminate them.[518] In exchange for their complete testimony, they receive immunity against compelled evidence being used in subsequent proceedings to incriminate them. The immunity offered by these provisions is of testimonial nature only and does not extend to evidence that exists independently of the testimony, even if this evidence was obtained following the testimony and is consequently *derivative* by its nature.[519] In other words, s. 5 of the *Canada Evidence Act* and s. 13 of the *Charter* do not grant *derivative use* immunity to witnesses. Derivative use immunity has been rather found to be granted by s. 7 of the *Charter.*[520]

The majority in *Thomson Newspapers* concluded that the principle against self-incrimination did not justify "an absolute rule that testimonial immunity must always extend to evidence derived from compelled testimony,"[521] mostly because derivative evidence by definition exists independently of the compelled testimony, making it discoverable without the participation of the witness. In that sense, derivative evidence only implicates self-incrimination "by virtue of the circumstances of [its] discovery in a particular case."[522] The majority thus concluded that derivative use immunity should only be granted when the use of the evidence derived from compelled testimony would undermine the fairness of the trial.

Building on these findings from *Thomson Newspaper*, the SCC in *R v S (RJ)* revisited the scope of the different immunities granted by the *Charter*. According to the majority,

---

[518] According to *Kuldip*, *supra* note 357 at 642, s. 5(2) and of the *Canada Evidence Act* and s. 13 of the *Charter* offer virtually the same protection, by way of immunity against compelled self-incrimination.
[519] *S (RJ)*, *supra* note 343 at paras 161–164, 172–173.
[520] *BC Securities*, *supra* note 376 at paras 2-7, building on *S (RJ)*, *supra* note 343.
[521] *Thomson Newspapers Ltd v Canada*, *supra* note 345 at 548–549.
[522] *Ibid* at 550. This will become important when it comes to the application of the principle against self-incrimination to compelled decryption. Indeed, compelled decryption, like derivative evidence, becomes available to the prosecution by way of compulsion. See Section 7.1.2(B) *infra*.

derivative evidence can only be qualified as being truly derivative when it effectively results from a compelled disclosure; any other evidence that is discovered independently from the compelled testimony does not implicate the principle against self-incrimination.[523] To reach the conclusion that not all derivative evidence will be protected by way of immunity, the majority examined the American experience with immunities, as well as the SCC's jurisprudence on s. 24(2) of the *Charter*. Considering that not all evidence obtained in violation of the *Charter* is excluded under s. 24(2), it follows that the admission of derivative evidence will not always be contrary to the principles of fundamental justice, as saying otherwise would mean that "the admission of evidence which offends the principles of fundamental justice does not bring the administration of justice into disrepute".[524] Such conclusion is untenable in the context of the *Charter* and of trial fairness.

The jurisprudence on s. 24(2) of the *Charter* until *R v S (RJ)* also informs us that evidence will be considered to be self-incriminating when it was "manifestly created by an accused (such as a pre-trial statement), but also any evidence which could not have been obtained by the state from the accused but for the *Charter* violation."[525] This was found by Iacobucci J. as being determinative when it comes to the question of derivative use immunity, *inter alia* because the *Charter* should be interpreted in a coherent manner. As such, derivative evidence that could not have been obtained, or which the significance could not have been appreciated, *but for* the compelled participation of the witness should not be allowed into evidence and

[523] *S (RJ)*, *supra* note 343 at para 165. Or as described by Wilson J. in *Thomson Newspapers Ltd v Canada*, *supra* note 345 at 484, there must be a "direct causal relationship between the compelled testimony and the derivative evidence," for it to be qualified as such.
[524] *S (RJ)*, *supra* note 343 at para 177.
[525] *Ibid* at para 189.

ought rather to be excluded under s. 7, as its admission would render the trial unfair.[526] This conclusion holds true regardless of whether the accused *created* the evidence or not, which means that evidence that is not self-incriminatory by its creation can still be considered as such by way of its discovery by the state.[527]

The determination of the application of this residual derivative-use immunity in a specific case will need to be determined in the subsequent proceeding in which the prosecution seeks to introduce the derivative evidence against the witness that gave the testimony.[528] For this reason, the majority in *R v S (RJ)* left the door open to subsequent interpretation of what the concrete application of this test should look like but did make comments of a general nature. Most importantly, Justice Iacobucci underlined that derivative use immunity should be granted when the evidence could not have been located by the authorities absent of the compelled testimony following "logical probabilities, not mere possibilities."[529]

The same year, the Court re-examined the "but for" test from *R v S (RJ)* in *British Columbia Securities Commission v Branch*. In this decision, the Court restated that the "but for" test only applies in subsequent procedures, when the initial testimony has already been given. Accordingly, the "but for" test does not apply to determine the compellability of a witness (or the compellability of documents). In that sense, it "takes over where [s. 5(2) of the *Canada Evidence Act*] leaves off providing greater use immunity,"[530] but both protections are

[526] It should be noted however that following *Grant*, derivative evidence will not automatically be excluded under s. 24(2) of the Charter. *Grant*, *supra* note 434 at paras 116–128.
[527] *S (RJ)*, *supra* note 343 at para 191.
[528] *Ibid* at para 192.
[529] *Ibid* at para 195.
[530] *BC Securities*, *supra* note 376 at para 42.

applicable under the same circumstances, i.e., after the witness has indeed provided the evidence, whether of testimonial or material nature.[531]

When it comes to real evidence, the same principles apply. Accordingly, the *Charter* does not protect against the compelled production of documents (or other material evidence), but only against their subsequent use to incriminate the witness compelled to produce them. While pre-existing documents do not directly implicate the principle against self-incrimination, the act of producing documents can sometime have communicative aspects, such as inferences of knowledge or truth of the contents, which can be of significance under the "but for" test.[532]

The burden of proof applicable to derivative use immunity rests on the accused who claims that s. 7 of the *Charter* would be infringed if the evidence was admitted. In order for the immunity to apply, the accused will need to establish, on a balance of probabilities, that the evidence emanates from the compelled testimony. The Crown will then have the opportunity to establish, once again on a balance of probabilities, that the authorities would have discovered the impugned derivative evidence absent the compelled testimony.[533] Derivative use immunity (as well as use immunity) will also be applicable when a privileged statement is disclosed as part of a *McClure* application, applicable to obtain the production of privileged documents relating to communications between an individual and their lawyer, as the privilege holder will indirectly have been compelled to self-incriminate.[534]

---

[531] Other provisions may grant similar protections in specific situations. For example, the SCC in *Application under s. 83.28 of the Criminal Code (Re)*, *supra* note 378 at para 72 determined that s. 83.28(10) of the *Criminal Code*, before being repelled in 2019, provided for both use and derivative use immunity.
[532] *BC Securities*, *supra* note 376 at paras 45–48.
[533] *S (RJ)*, *supra* note 343 at para 202; *BC Securities*, *supra* note 376 at para 5.
[534] *Brown*, *supra* note 416 at para 99.

In light of the above, it seems clear that compelled decryption will implicate the principle against self-incrimination, as it removes the *choice* that individuals have to collaborate or otherwise engage with the authorities. However, and as mentioned, the dual nature of compelled decryption, which gives the state access to both testimonial and non-testimonial evidence, will need to be factored into the determination of the specific application of the principle against self-incrimination to this unique investigative technique. Further, use and derivative use immunity, generally used to alleviate the impacts of coercive procedures on the principle against self-incrimination during the trial phase of the criminal process, will prove useful to mitigate the impact of compelled decryption on the testimonial aspect of the act of decryption, which is an assertion of the ability to decrypt and an assertion of control over the data or device.

CHAPTER 5 THE RIGHT TO PROTECTION FROM UNREASONABLE SEARCH AND SEIZURE

The Supreme Court of Canada started its analysis of s. 8 of the *Charter,* which protects against unreasonable search and seizure, in 1984—two years after the adoption of the constitutional document—in *Hunter et al. v Southam Inc*.[535] In *Hunter*, the Court outlined the premises of the protection against unreasonable search and seizure and began what would become a long lineage of s. 8 jurisprudence.

Since then, search and seizure principles have been explored regularly by the courts and scholars alike. It is fair to say that search and seizure law has received more attention than the principle against self-incrimination throughout the years. The interplay between the two protections has received even less attention, probably because ss. 7 and 8 are often seen as being mutually exclusive. However, in the context of encryption and electronic devices, both protections become interwoven, making the study of both essential in order to determine what compelled decryption can look like in Canada.

The focus of this chapter will be on the evolution of the s. 8 jurisprudence as the courts grappled with the problems raised by electronic devices and evidence.[536] The notion that this protection, alongside the privilege against self-incrimination, was meant to limit state power, not augment it, will be analyzed.[537] The various judicial authorizations applicable to the search

[535] *Hunter*, *supra* note 31.
[536] Including *Morelli*, *supra* note 30; *Cole*, *supra* note 30; *TELUS*, *supra* note 249; *Vu*, *supra* note 1; *Spencer*, *supra* note 241; *Fearon*, *supra* note 1; *Jones II*, *supra* note 249; *Marakah*, *supra* note 260; *Reeves*, *supra* note 250; *Mills II*, *supra* note 264.
[537] Bryan H Choi, "For Whom the Data Tolls: A Reunified Theory of Fourth and Fifth Amendment Jurisprudence" (2015) 37 Cardozo L Rev 185.

and seizure of information will also be reviewed, alongside the exceptional warrantless search and seizure powers available to law enforcement. These general principles will be applied to compelled decryption subsequently, in Part 2. It should be kept in mind that this chapter does not seek to paint a complete portrait of search and seizure law conceived broadly, since this inquiry would be too burdensome for this thesis' purpose. Instead, only what is relevant to the specific exploration of compelled decryption and unlocking of devices will be considered.

5.1 The Application of s. 8 of the Charter in an Analog World

5.1.1 The Structure, Purpose and General Principles Applicable to s. 8 of the Charter

> *Everyone has the right to be secure against unreasonable search or seizure.*[538]

As noted, the *Charter* does not contain an explicit protection for privacy, conceived broadly. Instead, s. 8 of the *Charter* has been interpreted as protecting *reasonable expectations of privacy* against *unreasonable* searches and seizures. This puts the notion of reasonableness at the center of the analysis.[539] Effectively, the constitutional protection of privacy does not prohibit the state from interfering with privacy interests; rather, it provides ground rules that must be respected by the state when it uses investigative techniques that impact reasonable expectations of privacy, on the basis that imposing restraints on governmental action is essential in a democratic state.[540] Like any other *Charter*-protected right then, the right to

[538] *Charter*, *supra* note 24, s 8.
[539] As was demonstrated in Chapter 3, defining privacy is difficult. As such, the determination of what is reasonable under s. 8 can also be quite difficult. See *inter alia Tessling*, *supra* note 250 at para 25.
[540] *Dyment*, *supra* note 291 at 427–428.

privacy is not absolute.[541] Conversely, "the state's interest in acquiring evidence is [also] not absolute."[542]

Interpreting s. 8 should "emphasize the protection of privacy as a prerequisite to individual security, self-fulfilment and autonomy as well as to the maintenance of a thriving democratic society."[543] The SCC has also left the door open to the possibility that s. 8 protects interests other than privacy, including the right against self-incrimination.[544] It must also be kept in mind that individuals not only have an interest into keeping certain things private, but also in staying safe from crimes committed by other people.[545]

The words "search" and "seizure" are used disjunctively in s. 8 of the *Charter*, which means that in some cases the search of a subject matter can be reasonable but not its seizure, and vice versa.[546] A seizure can be defined as "the taking of a thing from a person by a public authority without that person's consent."[547] "Search" is a more loosely defined term and will involve multiple types of state action that encroach upon a reasonable expectation of privacy, such as the search of a house for evidence, the search of an accused's person and personal belongings incident to arrest, or the search of the contents of an electronic device.

Generally speaking, the *Charter* aims "to guarantee and to protect, within the limits of reason, the enjoyment of the rights and freedoms it enshrines."[548] As such, s. 8 aspires to limit

---

[541] *Gomboc*, *supra* note 291 at para 17.
[542] *Fearon*, *supra* note 1 at para 154.
[543] *Spencer*, *supra* note 241 at para 15.
[544] *Hunter*, *supra* note 31 at 159; *SAB*, *supra* note 430 at para 35.
[545] *Tessling*, *supra* note 250 at para 17.
[546] *Dyment*, *supra* note 291 at 431.
[547] *Ibid*.
[548] *Hunter*, *supra* note 31 at 156.

governmental action, not enable it, even when it comes to reasonable searches and seizures.[549] Law enforcement requires legal foundations to justify the existence of investigatory techniques that qualify as searches or seizures, whether in the common law or from statutory sources. Section 8 also has a preventative function, by not only prohibiting unreasonable searches and seizures, but by also guaranteeing the right to be secure from them.[550] The state should then strive to standardize methods of interfering with citizens' rights and prevent unreasonable searches by providing guidance for law enforcement, ensuring that investigatory powers are carried out in a reasonable manner.[551]

Concretely, to give effect to the preventative goal of s. 8, a system of prior authorization is necessary, except in some specific situations.[552] Accordingly, a prior judicial authorization signed by a judge or someone acting judicially will usually be necessary if law enforcement wants to carry out a technique that encroaches on a reasonable expectation of privacy. If that is not the case, the search or seizure carried out without prior authorization will be presumed unreasonable and the party seeking to introduce into evidence the results of such search or seizure will need to rebut this presumption of unreasonableness,[553] often by invoking a common law warrantless search power.

The standard applicable to the issuance of prior judicial authorization will usually be that of "reasonable grounds to believe," although newer provisions in the *Criminal Code* now allow

---

[549] *Ibid* at 156–157. Or as put by the SCC in *R v Big M Drug Mart*, [1985] 1 SCR 295 at 336: "One of the major purposes of the Charter if to protect, within reason, from compulsion or restraint."
[550] *Hunter*, *supra* note 31 at 160; *Dyment*, *supra* note 291 at 427.
[551] *Ibid* at 430. See also Zarefsky, *supra* note 331 at 183 on the standardization aspect of the Fourth Amendment, the American equivalent to s. 8.
[552] *Hunter*, *supra* note 31 at 160–161. See Section 5.5 *infra*.
[553] *Ibid* at 161; *Cole*, *supra* note 30 at para 37; *R v Nolet*, 2010 SCC 24, [2010] 1 SCR 851 at para 21.

the issuance of some authorizations under the standard of "reasonable ground to suspect." The applicable standard, whether of "reasonable grounds to believe" or "reasonable grounds to suspect," allows for law enforcement considerations to be properly balanced against individuals' privacy rights,[554] which is also an important goal s. 8 itself strives to accomplish.[555] In other words, "[t]he state's interest in detecting and preventing crime begins to prevail over the individual's interest in being left alone at the point where credibly-based probability replaces suspicion."[556] The prior authorization requirement also furthers the goal of balancing the state interest in investigating and prosecuting crime against the right of the individual to be free from state interference, as it puts the onus on the state to demonstrate the superiority of its interest.[557]

From the start, the SCC has made it clear that s. 8 does not only protect what was traditionally protected by the common law protection regarding governmental searches and seizures. Prior to the advent of the *Charter*, the common law protection was indeed fairly limited as it was directly correlated with property and with the law of trespass.[558] Section 8, the Court has often said, serves a larger purpose by protecting people, not places.[559] As such, the Court's jurisprudence has refined the protection against unreasonable search and seizure to cover three

[554] *Hunter*, *supra* note 31 at 167–168.
[555] *Ibid* at 159–160, 167–168; *Dyment*, *supra* note 291 at 428.
[556] *Hunter*, *supra* note 31 at 167.
[557] *Ibid* at 160.
[558] *Ibid* at 157–158.
[559] *Ibid* at 159, referring to the United States Supreme Court decision in *Katz v United States*, 389 U.S. 347 (1967) at 351.

zones or realms of privacy: (1) territorial privacy; (2) personal privacy; and (3) informational privacy.[560] In a specific instance, the different zones of privacy can interact and overlap.[561]

Territorial privacy, as its name indicates, is concerned about specific places where individuals can reasonably expect privacy, such as homes, private offices, or, to a lesser degree, cars. This zone of privacy is still linked to property to some extent, but ownership is only one of the relevant considerations to the establishment of a reasonable expectation of territorial privacy.[562] The human body is the main object of personal privacy and this zone of privacy will come into play in such instances as bodily (frisk) searches or seizure of bodily substances. Searches and seizures involving a suspect's body are generally seen as highly invasive, as they constitute an affront to human dignity by violating the sanctity of a person's body.[563] Finally, informational privacy also relates to human dignity as individuals should be free to communicate or retain information about themselves as they see fit.[564] The type of information protected is biographical core information, which is information that "tends to reveal intimate details of the lifestyle and personal choices of the individual."[565] The SCC has specified that informational privacy includes at least "three conceptually distinct although overlapping understandings of privacy: as *secrecy*, as *control*, and as *anonymity*."[566]

---

[560] *Dyment*, *supra* note 291 at 428.
[561] *Tessling*, *supra* note 250 at para 24.
[562] *Edwards*, *supra* note 235 at para 45; *Cole*, *supra* note 30 at para 51; *Reeves*, *supra* note 250 at para 39. See also Section 5.1.2 immediately *infra*.
[563] *Dyment*, *supra* note 291 at 429.
[564] *Ibid* at 429–430. Or as Westin, *supra* note 239 at 7 puts it, privacy rests on "the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain...as he sees fit." (as cited in *Tessling*, *supra* note 250 at para 23 *in fine*).
[565] *R v Plant*, [1993] 3 SCR 281 at 293 [*Plant*]; *Tessling*, *supra* note 250 at paras 25–26.
[566] *Spencer*, *supra* note 241 at para 38, as paraphrased in *Mills II*, *supra* note 264 at para 21.

5.1.2 The Reasonable Expectancy of Privacy Test

The existence of a reasonable expectation of privacy is a threshold condition that determines if s. 8 in triggered in the first place. The totality of the circumstances must be considered to determine if a reasonable expectation of privacy was present in a specific case.[567] Without a reasonable expectation of privacy, the state's action will not qualify as a search and seizure, making its usage by the authorities entirely discretionary and not reviewable by the courts under s. 8 of the *Charter*.[568] In other words, "only where those state examinations constitute an intrusion upon some reasonable expectation of privacy interest of individuals does the government action in question constitutes a "search" within the meaning of s. 8."[569]

To determine if a reasonable expectation of privacy is present, courts follow a four-step analysis that was set out by the SCC in *Tessling*[570] and used consistently ever since.[571] This "totality of the circumstances" test follows four lines of inquiry:

> (1) an examination of the subject matter of the alleged search; (2) a determination as to whether the claimant had a direct interest in the subject matter; (3) an inquiry into whether the claimant had a subjective expectation of privacy in the subject matter; and (4) an assessment as to whether this subjective expectation of privacy was objectively reasonable, having regard to the totality of the circumstances.[572]

---

[567] *Edwards*, *supra* note 235 at para 45; *R v Colarusso*, [1994] 1 SCR 20 at 54 [*Colarusso*]; *R v Wong*, [1990] 3 SCR 36 at 62 [*Wong*]; *Spencer*, *supra* note 241 at para 17.
[568] *Gomboc*, *supra* note 291 at para 20 *in fine*; *Kang-Brown*, *supra* note 229 at para 161.
[569] *R v Evans*, [1996] 1 SCR 8 at para 11 [*Evans*].
[570] *Tessling*, *supra* note 250 at para 32 paraphrasing the analysis set forth in *Edwards*, *supra* note 235 at para 45.
[571] See inter alia *R v Patrick*, 2009 SCC 17, [2009] 1 SCR 579 [*Patrick*] at para 27; *Cole*, *supra* note 30 at para 40; *Spencer*, *supra* note 241 at para 18; *Marakah*, *supra* note 260; *Jones II*, *supra* note 249; *Reeves*, *supra* note 250; *Mills II*, *supra* note 264 at para 13.
[572] *Cole*, *supra* note 30 at para 40.

The analysis is not simply fact-based, as the protection afforded by s. 8 is normative, rather than purely descriptive.[573] The determination of what is reasonable to expect when it comes to individual privacy is consequently "laden with value judgments which are made from the independent perspective of the reasonable and informed person who is concerned about the long-term consequences of government action for the protection of privacy."[574] It implies looking at what society has come to expect regarding the specific privacy interest at play.[575]

Further, privacy in the context of s. 8 is not an "all-or-nothing" concept, which means that even a reduced reasonable expectation of privacy will attract protection under s. 8,[576] in a manner that is correlative with the strength of the privacy interest at play. As mentioned, this may mean that the applicable standard to obtain a judicial authorization will be lower than the usual "reasonable grounds to believe" standard, or that law enforcement will be allowed to conduct the search or seizure without prior judicial authorization, using a common law power.

In many cases, the individual claiming the protection of s. 8 of the *Charter* will be the person whose privacy rights have been most directly infringed by the authorities (e.g., the accused is the owner of the house which was illegally intruded upon by the authorities and where the contested search took place).[577] However, this will not always be the case. Indeed, if an accused satisfies the "totality of circumstances test," they will have the necessary "standing"

---

[573] *Tessling*, *supra* note 250 at para 42; *Spencer*, *supra* note 241 at para 18; *Patrick*, *supra* note 571 at para 14.
[574] *Patrick*, *supra* note 571 at para 14, cited in *Spencer*, *supra* note 241 at para 18. See also *Jones II*, *supra* note 249 at para 45; *Jarvis II*, *supra* note 263 at para 60; *Mills II*, *supra* note 264 at para 20.
[575] For example, in *R v Buhay*, 2003 SCC 30, [2003] 1 SCR 631 at para 19 [*Buhay*], the SCC examined "whether in a society such as ours persons who store and lock belongings in a bus depot locker have a reasonable expectation of privacy."
[576] *Jarvis II*, *supra* note 263 at para 61.
[577] See *inter alia Edwards*, *supra* note 235 at para 34, where Cory J. specified that "the privacy right allegedly infringed must, as a general rule, be that of the accused person who makes the challenge."

to contest the legally of a search or seizure, even if their privacy rights are maybe less obvious. This has led the SCC in *Marakah* and *Jones*, for example, to conclude that an accused has the necessary standing to challenge the legality of a search that first and foremost impacted their co-accused's privacy rights, if the prosecution is trying to introduce into evidence the result of that search.[578]

For clarity purposes, it is worth exploring each of the four lines of inquiry separately.

A) The Subject Matter of the Alleged Search

The identification of the subject matter of the search will usually be relatively straightforward except, as will be shown in section 5.2, when it comes to newer technologies. In any case, what is important is to look at what the police officers are actually trying to obtain, without focusing unnecessarily on the police conduct itself. In other words:

> As Doherty J.A. stated in *R. v. Ward*, 2012 ONCA 660, 112 O.R. (3d) 321, at para. 65, a court identifying the subject matter of a search must not do so "narrowly in terms of the physical acts involved or the physical space invaded, but rather by reference to the nature of the privacy interests potentially compromised by the state action". In *Spencer*, at para. 26, Cromwell J. endorsed these words and added that courts should take "a broad and functional approach to the question, examining the connection between the police investigative technique and the privacy interest at stake" and should look at "not only the nature of the precise information sought, but also at the nature of the information that it reveals". The court's task, as Doherty J.A. put it in *Ward*, is to determine "what the police were really after" (para. 67).[579]

[578] *Jones II*, *supra* note 249; *Marakah*, *supra* note 260. See also *infra* on both these decisions.
[579] *Marakah*, *supra* note 260 at para 15.

For example, the SCC in *Tessling* determined that the subject matter of a Forward Looking Infra-Red ("FLIR") image search was the pattern of heat emanating from a structure,[580] in *Kang-Brown* it concluded that the subject matter of a sniffer-dog search is the content of the bag (rather than the public airspace surrounding the bag),[581] and in *Patrick*, that searching garbage bags is effectively a search of information potentially contained in the bags.[582]

R v Saeed is a good example of the difficulty that can arise at this step (even in non-digital settings) as the SCC judges did not agree on the qualification of the subject matter of the search. In this case, the accused was subjected to a warrantless penile swab in the course of a sexual assault investigation. Writing for the majority, Justice Moldaver's held that the subject matter of the search was the complainant's DNA, found on the accused's penis.[583] In her dissenting reasons, Justice Karakatsanis decided that it was impossible to avoid the fact that the seizure implicated the accused's genital area and would inevitably also collect a sample of his own DNA.[584]

When it comes to digital information, *Spencer*, *Marakah, Jones*, and *Reeves* exemplify the importance of properly identifying the subject matter of the search.[585] By focusing on what law enforcement is truly seeking, these four cases demonstrate that the proper identification of the subject matter of the search must reflect the underlying information that can be revealed to the authorities by the search or seizure. Accordingly, when law enforcement is obtaining subscriber information linked to an IP address, they are not only obtaining the name and

---

[580] *Tessling*, *supra* note 250 at paras 34–36.
[581] *Kang-Brown*, *supra* note 229.
[582] *Patrick*, *supra* note 571 at para 30.
[583] *R v Saeed*, 2016 SCC 24, [2016] 1 SCR 518 at para 45 [*Saeed*].
[584] *Ibid* at 101–104. Abella J. agreed with Karakatsanis' s. 8 analysis.
[585] These cases will be examined in more details in Section 5.2 *infra*.

physical location of the subscriber, but also that subscriber's particular internet usage;[586] when obtaining text messages from a device or a telecommunication service provider, the subject of the search is the electronic conversation that occurred between the sender and the recipient(s), not only the copy of the text message in itself;[587] and when searching a computer, the subject matter of the search is ultimately the data contained within the device, not merely the physical device itself.[588]

B) The Existence of a Direct Interest in the Subject Matter

This requirement is strongly linked to the following one, as people who have a direct interest in the subject matter will usually also have a subjective expectation of privacy towards that same subject matter. Possession or ownership will usually be sufficient to demonstrate a direct interest in the subject matter, but a specific kind of usage can also be sufficient, regardless of actual ownership.[589]

C) The Existence of a Subjective Expectation of Privacy

The determination of a subjective expectation of privacy is necessarily factual but it is not a very stringent requirement to meet.[590] The opposite could "not be reconciled with the normative nature of the s. 8 inquiry."[591] As the SCC has held, the idea that we now live in a surveillance society (and thus have a reduced *subjective* expectation of privacy) should not be

[586] *Spencer*, *supra* note 241 at para 32.
[587] *Marakah*, *supra* note 260 at para 19; *Jones II*, *supra* note 249 at para 14.
[588] *Reeves*, *supra* note 250 at para 30.
[589] *Cole*, *supra* note 30 at para 43. See for example, *Jones II*, *supra* note 249, where the requirements were treated as one by the SCC.
[590] *Marakah*, *supra* note 260 at para 22; *Patrick*, *supra* note 571 at para 37; *Jones II*, *supra* note 250 at para 20.
[591] *Jones II*, *supra* note 249 at para 20.

used to lower the constitutional protection offered by the *Charter*.[592] Accepting this conclusion would render the protection of s. 8 meaningless.

In order to meet this requirement, the claimant will be able to rely on the prosecution's theory of the facts.[593] This means that, for example, in *Jones II*, the claimant was able to establish he had a subjective expectation of privacy in text messages found on a third party's phone (and a direct interest in the text messages), without admitting that he was the author of the messages and without testifying during the *voir dire*.[594]

This exception to the principle that the claimant "bears the burden of persuading the court that [their] *Charter* rights or freedoms have been infringed or denied"[595] is justified for multiple reasons. Most interestingly for our purposes, Côté J, in *Jones II*, explicitly mentioned that the opposite would "[sit] uneasily alongside the principle against self-incrimination."[596] Justice Côté recognized that, while not a free-standing legal principle, the principle against self-incrimination is applicable when it comes to the interpretation and to the creation of legal rules.[597] As such, the SCC now recognizes that placing accused individuals in a "catch-22," where they can either admit their individual relationship with the subject matter of the search in order to claim *Charter* protection, or sacrifice the ability to deny their responsibility at the trial itself, is not acceptable when we properly consider the privacy and self-incrimination interests at play.[598]

---

[592] *Tessling*, *supra* note 250 at para 42.
[593] *Jones II*, *supra* note 249 at paras 9, 18–19.
[594] *Ibid* at para 34.
[595] *R v Collins*, *supra* note 31 at 277.
[596] *Jones II*, *supra* note 249 at para 29.
[597] *Ibid* at para 30.
[598] *Ibid* at para 18.

D) The Reasonableness of the Subjective Expectation of Privacy

To determine if a subjective expectation of privacy is objectively reasonable, the totality of the circumstances must be considered. Over the years, multiple factors have been used by the courts, including the following factors from *Tessling*:

> a. the place where the alleged "search" occurred;
>
> b. whether the subject matter was in public view;
>
> c. whether the subject matter had been abandoned;
>
> d. whether the information was already in the hands of third parties; if so, was it subject to an obligation of confidentiality?
>
> e. whether the police technique was intrusive in relation to the privacy interest;
>
> f. whether the use of surveillance technology was itself objectively unreasonable.[599]

In *Marakah*, the SCC focused its analysis on three main factors to determine if the subjective expectation of privacy of the accused in the text messages recovered from his accomplice's phone was objectively reasonable: the place where the search occurred, the private nature of the subject matter, and control over the subject matter.[600] The majority restated that no factor is determinative by itself, especially considering that most factors were crafted in an analog era, which makes them hard to apply when it comes to a digital subject matter. On the private nature of the subject matter, the Court mentioned that information will normally attract a reasonable expectation of privacy when the search or seizure has "the potential for revealing

[599] *Tessling*, *supra* note 250 at para 32.
[600] *Marakah*, *supra* note 260 at para 24.

private information."[601] Privacy interests may also emerge from the simple existence of the information sought-after by law enforcement.[602]

The information that the investigative technique is susceptible of revealing must therefore be examined, but not every technique that allows the police to draw inferences of criminal activity will be protected against.[603] For that to be the case, the technique must be seeking "biographical core data".[604] Put differently:

> The closer the subject matter of the alleged search lies to the biographical core of personal information, the more this factor will favour a reasonable expectation of privacy. Put another way, the more personal and confidential the information, the more willing reasonable and informed Canadians will be to recognize the existence of a constitutionally protected privacy interest.[605]

The factor of control has historically been very important in the determination of the existence of a reasonable expectation of privacy.[606] However, decisions such as *Duarte* and *Marakah* have highly nuanced the application of this factor. Pursuant to these decisions, the risk that a third party that has access to the subject matter of the search would decide to disclose its existence to the authorities does not relinquish the control that the claimant has on the subject matter of the search (and thereby make the claimant's subjective expectation of privacy unreasonable).[607] The fact that the claimant shares control over the subject matter of the search

---

[601] *Ibid* at para 31. See also *Gomboc*, *supra* note 291 at paras 34–35.
[602] *Marakah*, *supra* note 260 at para 33.
[603] *Gomboc*, *supra* note 291 at para 38.
[604] *Ibid* at paras 34, 39.
[605] *Cole*, *supra* note 30 at para 46.
[606] *Marakah*, *supra* note 260 at para 38.
[607] In *R v Duarte*, [1990] 1 SCR 30 [*Duarte*] the Court examined whether co-conversationalists retain a reasonable expectation of privacy by having a conversation, while in *Marakah*, *supra* note 260 at paras 40–42, the Court examined whether digital conversation could be treated in the same manner.

is then not fatal to the recognition of a reasonable expectation of privacy.[608] Similarly, the fact that information has been shared with a third party will not necessarily mean that the information cannot attract a reasonable expectation of privacy.[609] The crux of the matter will be to determine if the subject of the search was worthy of protection, with regard to all relevant circumstances.

Importantly, the recognition of a reasonable expectation of privacy is content neutral and should not be impacted by the nature of the activities or information for which the claimant seeks protection under s. 8. As such, the criminal nature of the subject matter of the search should not be an obstacle to the recognition of a reasonable expectation of privacy.[610] In other words, an *ex post facto* confirmation of criminal activity cannot negate a reasonable expectation of privacy.[611]

Items that have been abandoned will usually not be the subject of a reasonable expectation of privacy.[612] The same can be said of objects or actions voluntarily and knowingly exposed to the public,[613] within the limit of what we expect and allow as a society for third parties to do

[608] See also *Reeves*, *supra* note 250; *Cole*, *supra* note 30.
[609] *Spencer*, *supra* note 241.
[610] *Marakah*, *supra* note 260 at para 48; *Gomboc*, *supra* note 291 at para 39; *Spencer*, *supra* note 241 at para 36; *Mills II*, *supra* note 264 at para 25. The majorities decision in *Mills II* however has been criticized for not truly providing a content-neutral approach. See Martin J.'s dissenting motives, at para 110.
[611] *Wong*, *supra* note 567 at 49–50.
[612] *Patrick*, *supra* note 571 at para 73; *Dyment*, *supra* note 291 at para 22; *Stillman*, *supra* note 353 at para 23.
[613] *Tessling*, *supra* note 250 at para 40; *Stillman*, *supra* note 353 at para 62; *Evans*, *supra* note 569 at para 50; *Dyment*, *supra* note 291 at 435.

with what is exposed.[614] The contractual and statutory frameworks applicable to a specific subject matter may also be considered—but will not be determinative.[615]

5.1.3 The Reasonableness of the Search or Seizure

Reasonableness is not only relevant as the threshold condition of establishing the existence of a reasonable expectation of privacy. As the text of s. 8 indicates, the search or seizure itself must also be reasonable. The SCC has interpreted this reasonableness condition as applying at three separate levels: "[a] search will be reasonable if it is authorized by law, if the law itself is reasonable and if the manner in which the search was carried out is reasonable."[616]

A) The Presence of a Lawful Authorization

The lawful authorization can come from statutory sources, or from common law powers.[617] Determining if a common law power allows for such police intervention will sometimes be fairly straightforward, when the common law power is widely recognized as such. For example, it is commonly accepted that the common law grants the police the power to search a suspect incident to arrest.[618]

---

[614] For example, in *Jarvis II*, *supra* note 263, the Court made the distinction between appearing in public (which is not subject to a reasonable expectation of privacy) and being recorded in public (which can sometimes be subject of a reasonable expectation of privacy). While the Court in *Jarvis II* examined the concept of privacy in the context of the offence of voyeurism, this comment is applicable when it comes to the interpretation of s. 8.
[615] *Spencer*, *supra* note 241 at para 54; *Gomboc*, *supra* note 291 at paras 31–32. Similarly, the commercial nature of the relationship between the claimant and the third party holding the information will not necessarily foreclose a s. 8 claim but may it be considered. See *Plant*, *supra* note 565 at 294.
[616] *R v Collins*, *supra* note 31 at 278.
[617] *R v Wiley*, [1993] 3 SCR 263 at 273; *R v Caslake*, [1998] 1 SCR 51 at para 30 [*Caslake*]; *Buhay*, *supra* note 575 at para 35; *Stillman*, *supra* note 353 at para 25.
[618] *Fearon*, *supra* note 1 at para 14.

However, in other cases, the common law power will not be so easily identified. In those cases, the courts will sometimes use the ancillary powers doctrine (also called the *Waterfield* test).[619] According to this doctrine, law enforcement officers will be authorized by common law to interfere with individual freedom or liberties if "(1) the police were acting in the course of their duty, when they effected that interference, and (2) the conduct of the police did not involve an unjustifiable use of powers in the circumstances."[620] The second step of the analysis is subsumed in the third prong of the *Collins* test, as it requires examining if the search was reasonably necessary, in the specific instance being considered.[621]

Generally, police duties under this test will include "solv[ing] crime and bring[ing] the perpetrators to justice,"[622] preserving social peace, preventing crime, and protecting life and property.[623] The preservation of highly reliable evidence, as well as the fact that the search could serve to exclude an innocent suspect, have also been qualified as important law enforcement objectives.[624] It is also possible to refer to provincial statutes to determine the duties of police officers.[625]

---

[619] The SCC in *Fleming v Ontario*, 2019 SCC 45, [2019] 3 SCR 519 at para 43 mentions that the "ancillary powers doctrine" terminology should be preferred because it better reflects the fact that *R v Waterfield*, 1963 All ER 659 (English Court of Criminal Appeals) was not about the creation of a new police power but rather examined the question of whether a certain police officer had been acting in the execution of his duties in the case at bar. Accordingly, this thesis will use the "ancillary powers doctrine" terminology.

[620] *R v Godoy*, [1999] 1 SCR 311 at para 7 [*Godoy*]. This criterion is adapted from *Waterfield*, *supra* note 625. See also *Dedman*, *supra* note 453 at 35, cited in *Kang-Brown*, *supra* note 229 at para 49; *Cloutier v Langlois*, [1990] 1 SCR 158 at 181; *Fleming v Ontario*, *supra* note 619 at para 45; *R v Aucoin*, 2012 SCC 66, [2012] 3 SCR 408 at paras 73-75 [*Aucoin*].

[621] *R v Mann*, 2004 SCC 52 [2004] 3 SCR 59 at para 44 [*Mann*].

[622] *Kang-Brown*, *supra* note 229 at para 52.

[623] *Dedman*, *supra* note 453 at 11–12, cited in *Godoy*, *supra* note 620 at para 15. See also *Aucoin*, *supra* note 620 at para 74.

[624] *Saeed*, *supra* note 583 at paras 58–59.

[625] *Godoy*, *supra* note 620 at paras 14–15.

In applying the ancillary powers doctrine, judges should keep in mind that the common law has historically been perceived as a law of liberty.[626] Accordingly, the SCC was originally cautious when examining the possibility of interpreting common law powers in such way as to grant more power to the authorities.[627] More recently however, this seems to have changed. In decisions such as *Fearon*,[628] *Saeed*,[629] and *Stairs,*[630] a SCC majority concluded that warrantless search powers found in the common law should be modified and extended to allow for a broader reach, without waiting for Parliament to regulate the type of search being examined.

B) The Reasonableness of the Law Itself

Assessing the reasonableness of the authorizing provision allowing for a search or a seizure involves balancing the opposed interests of law enforcement and of citizens.[631] It requires the courts to examine the importance of the state objective, as opposed to the privacy interest identified previously.[632] Generally speaking, the higher privacy interests are in the subject matter of the search, the more stringent the conditions allowing for a search or seizure of that subject matter should be.[633] Keeping in mind that privacy is never absolute, the crux of the matter at this stage of the analysis will be to determine which conditions should be imposed on law enforcement, in order for them to obtain what they are seeking, while providing the adequate protection for the owner of the privacy right being affected. It should also be

[626] *Kang-Brown*, *supra* note 229 at para 12; *Cloutier v Langlois*, *supra* note 620 at 183.
[627] *Wong*, *supra* note 567 at 56–57.
[628] *Fearon*, *supra* note 1.
[629] *Saeed*, *supra* note 583.
[630] *R v Stairs*, 2022 SCC 11.
[631] *R v Rodgers*, 2006 SCC 15, [2006] 1 SCR 554 at para 27 [*Rodgers*].
[632] *Ibid*.
[633] *Gomboc*, *supra* note 291 at para 20; *Simmons*, *supra* note 490 at 517.

recognized that reasonable and probable grounds is the usual standard applicable in Canadian criminal law, whether it applies to a warrantless police power or to the issuance of a court authorization.[634] A lower standard, such as reasonable grounds to suspect should be reserved for cases where "the investigative technique is relatively non-intrusive and the expectation of privacy is not too high."[635]

The determination of what individuals can reasonably expect in terms of their privacy is highly contextual. For this reason, examining the reasonableness of the authorizing law must also be evaluated in context.[636] This means examining what the disputed provision is susceptible of providing to law enforcement, in the broader perspective of the state's interest in solving and preventing crime, protecting society, while respecting individuals' freedoms and rights.

In some instances, the privacy interest will be so negligible that conditions to validly carry out the search or seizure will be minimal. In *Rodgers*, for example, the SCC examined the reasonability of s. 487.055 of the *DNA Identification Act*, which allows for the collection of DNA samples of convicted persons. Justice Charron, writing for the majority, recognized that DNA samplings impact the privacy of convicted individuals by interfering with their physical integrity and by providing the state with private information.[637] However, she concluded that the provision was reasonable because the impact on the physical integrity of the subject is very minimal and because the information provided to the state can only be used in very

[634] *Kang-Brown*, *supra* note 229 at para 13.
[635] *Ibid* at para 168.
[636] *Rodgers*, *supra* note 631 at paras 26–27.
[637] *Ibid* at para 39.

limited ways—for identification purposes only.[638] Further, because the provision is applicable exclusively to a specific category of offenders, she concluded that the subject, having been convicted for violent offences, could not reasonably expect to remain anonymous towards the authorities.[639] For these reasons, she concluded:

> Having regard to the competing interests at play, I conclude that there is no constitutional requirement to link the convicted offender, on reasonable and probable grounds, to any particular investigation. The data bank provisions strike an appropriate balance between the public interest in the effective identification of persons convicted of serious offences and the rights of individuals to physical integrity and the right to control the release of information about themselves.[640]

In other cases, however, the privacy interests will be stronger, requiring more stringent conditions to be imposed to law enforcement in order to strike the appropriate balance. In *Golden*, the SCC modified the common law search incident to arrest standard to reflect the higher privacy interests encroached when police officers perform strip searches incident to arrest.[641] Similarly, in *Araujo*, the Court recognized that imposing stringent conditions on law enforcement officers seeking to obtain a wiretap authorization were necessary, because of their highly intrusive nature.[642]

Whether the power to search or to seize comes the common law or a statutory source, it will need to respect the *Charter*. Indeed, "[i]t has long been accepted that courts should apply and develop common law rules in accordance with the values and principles enshrined in the

---

[638] *Ibid* at para 42.
[639] *Ibid* at para 43.
[640] *Ibid* at para 44.
[641] *R v Golden*, 2001 SCC 83, [2001] 3 SCR 679 at para 97 [*Golden*].
[642] *R v Araujo*, 2000 SCC 65, [2000] 2 SCR 992 [*Araujo*].

Charter."[643] For this reason, even if a common law power is deemed to exist, the *Collins* test will still need to be applied in order to determine if that warrantless search or seizure power is constitutionally valid under s. 8 of the *Charter*.[644]

If a valid lawful authorization cannot be identified at step one, s. 1 of the *Charter* will not be applicable in order to try to save the search or seizure.[645]

C) The Manner in which the Search or Seizure is Carried Out

This last prong of the *Collins* test relates to how to search or seizure was effectively carried out by the authorities, in the specific case under review.[646] As mentioned, this is related to some degree to the second stage of the ancillary powers doctrine analysis.[647] It will require examining the totality of the circumstances, including whether law enforcement officials respected the applicable pre-conditions or guidelines before carrying out the search or seizure and whether the scope of the search and seizure was coherent with what law enforcement was seeking and with the privacy interest at stake.[648] Search and seizures need to be as minimally intrusive as possible in order to be carried out reasonably, with regard to the totality of the circumstances. This means that the use of physical force by the police may be reasonable in some contexts, but not in others.[649]

---

[643] *Rodgers*, *supra* note 631 at para 18; *Cloutier v Langlois*, *supra* note 620 at 184; *Golden*, *supra* note 641 at para 86; *Mann*, *supra* note 621 at paras 17–19; *RWDSU v Dolphin Delivery Ltd*, [1986] 2 SCR 573 at 603.
[644] *Mann*, *supra* note 621 at para 44.
[645] *R v Dersch*, [1993] 3 SCR 768 at 779.
[646] *R v Debot*, [1989] 2 SCR 1140 at 1148 [*Debot*].
[647] *Mann*, *supra* note 621 at para 44. See also *R v MacDonald*, [2014] 1 SCR 37 at para 47 [*MacDonald*].
[648] *MacDonald*, *supra* note 647 at paras 46–50.
[649] *Golden*, *supra* note 641. See also *R v Cornell*, 2010 SCC 31, [2010] 2 SCR 142, in which Binnie, Lebel and Fish JJ., in their dissenting motives, concluded that the dynamic entry was not necessary in the circumstances of the case, making the search carried out in an unreasonable manner.

5.2 The Evolution of s. 8 of the Charter in a Digital World

The SCC in Hunter not only built the foundations of the protection against unreasonable search and seizure but also did so in a way that allows for "growth and development over time to meet new social, political and historical realities."[650] The SCC has since then adapted the general principles from its earlier jurisprudence to meet the demands of new technology. As La Forest J. wrote:

> [T]he broad and general right to be secure from unreasonable search and seizure guaranteed by s. 8 is meant to keep pace with technological development, and, accordingly, to ensure that we are ever protected against unauthorized intrusions upon our privacy by the agents of the state, whatever technical form the means of invasion may take.[651]

While this comment referred to the advancements in the technology used by law enforcement, it can be applied *mutatis mutandis* to technology used by criminals, either to evade the authorities or to commit their crime directly.

This adaptation, however, has not always been easy or simple. Multiple factors can explain why courts, including the SCC, have historically struggled with new technologies. First, technological advancements are quick and difficult to predict, even for experts, due to their complex nature. Even recent decisions can now be perceived as outdated because the courts were not in a position to foresee how a specific technology would evolve in the near future.[652]

---

[650] *Hunter*, *supra* note 31 at 155.

[651] *Wong*, *supra* note 567 at 44.

[652] For example, *Spencer*, *supra* note 241 is now difficult to reconcile with the fact that so many electronic devices are now protected by encryption at the time of the suspect's arrest. The decision's reach is thus fairly limited, as the SCC did not address this problem even in obiter. Moreover, in *Tessling*, *supra* note 250 at para

Second, the nature of our adversarial justice system means that courts are very limited when it comes to requesting additional information on a specific subject, including the technological aspects of a case. The judge's role is of a neutral and impartial arbiter, not of an active participant in the criminal process, and there are limits on the extent to which judges can seek evidence to advance their understanding of technical points. This gap in judges' powers is amplified when it comes to complex technological contexts.[653] Third, time and resource constraints put on the criminal justice system do not allow for much flexibility when it comes to investigating certain questions in more depth. Individual parties suffer from these constraints, but also more generally the judiciary itself.[654] How can we possibly expect judges then to grasp such technical concepts or the parties to address all the possible ways a technology can evolve, in the fairly limited time allowed per case?

Further, the SCC has been inconsistent with the approach taken towards new technologies. Generally speaking, two opposing approaches (or models) have underpinned the examination of the impact of technology on criminal law, one that aims to maintain the historical equilibrium between privacy and security that existed prior to the development of the technology under review, and one that recognizes that technological advancements fundamentally shifted the relationship between privacy and security; respectively, the "technological neutrality" and "technological novelty" approaches, terminology coined by

29, the SCC mentioned that it is not necessary for the courts to try to foresee how a technology will evolve, making it necessary to address technological concerns on a piecemeal basis.

[653] See *inter alia* Colton Fehr, "Digital Evidence and the Adversarial System: A Recipe for Disaster?" (2018) 16 CJLT 437.

[654] One has to think only about *R v Jordan*, 2016 SCC 27, [2016] 1 SCR 631 [*Jordan*] to see how limited the criminal justice system can be.

Stephen Aylward.[655] "Technological neutrality" strives to regulate new technologies in a manner that is coherent with the equilibrium between privacy and public safety that existed prior to the advent of that technology, while "technological novelty" instead seeks to "recalibrate values of privacy and public safety to a new societal context."[656] These models reflect how technological changes can be examined through very different lenses, prompting outcomes that are in stark contrast to one another. While no model is 'wrong' or 'right' in itself, the issue here is that the SCC has used both of these models recently, thus creating a jurisprudence on privacy and technology that is not entirely coherent.[657]

Adopting an overarching model, or a strong interpretative preference, to guide lower courts in their decisions on digital privacy and the impact of technology on search and seizure law would prove helpful, especially in a context where, as mentioned, technological advancements are rapid and unpredictable, and where citizens should be able to be *protected* against unreasonable searches or seizures, instead of simply having a way to obtain redress after a s. 8 breach occurs. While waiting for Parliament to take action on certain specific topics—such as compelled decryption of data or unlocking of devices—guidance from the SCC on a general approach to take would help to correct the fact that courts generally struggle with new technologies.

---

[655] Stephen Aylward, "Technological Neutrality or Novelty? Two Models of Privacy in the Digital Era" (2017) 80 SCLR (2d) 423.

[656] *Ibid* at paras 6–7. The "technological neutrality" approach described by Aylward is very similar to what Kerr calls "equilibrium-adjustment theory." See Orin S Kerr, "An Equilibrium-Adjustment Theory of the Fourth Amendment" (2011) 125:2 Harv L Rev 476. The terminology coined by Aylward will be used in this thesis because of its Canadian origins.

[657] Aylward, *supra* note 655 puts *Fearon* in the "technological neutrality" category, and *Vu* and *Spencer* in the "technological novelty" category.

Before delving deeper in what that framework can look like in Part 2 of this thesis, this section will analyze how the SCC has dealt with cases involving computers and other electronic devices and how it tried to adapted itself and the law towards the new realities brought forward by these technologies. More specifically, the notion of reasonable expectation of privacy in devices and data will be analyzed directly below, while specific search and seizure powers will be examined in Section 5.3 *infra*.

5.2.1 The Existence of a Reasonable Expectation of Privacy in Data Found on Electronic Devices

The SCC first examined whether Canadians had a reasonable expectation of privacy towards their digital devices in *R v Morelli*.[658] In this case, a computer technician visiting the accused's house to install an internet connection concluded that the device had been used to view child pornography online, because of the name of website links that appeared on the screen when he was performing the work he was hired for.[659] Eventually, this information made its way to the authorities and a warrant was issued pursuant to s. 487 of the *Criminal Code*. The accused challenged the validity of the warrant at trial but was convicted by the trial judge. The conviction was upheld by the Court of Appeal for Saskatchewan.[660]

---

[658] *Morelli*, *supra* note 30.

[659] The specific circumstances at play in *Morelli* are not important here. However, it is worth mentioning that the computer technician who examined the accused's computer did not actually see illegal pornography on the screen, but rather deduced that the computer had been used to access such material *inter alia* because of the name of the links he saw on the screen. This, among other considerations, led the SCC to determine that the warrant had been illegally obtained by law enforcement, as the information to obtain (ITO) suggested that the technician had indeed seen child pornography on the screen and knew that it had subsequently been deleted by the accused. See *Morelli*, *supra* note 30, at paras 45-48.

[660] *Ibid* at paras 116–125 (as per Deschamps J., dissenting).

While the sufficiency (or deficiencies) of the information presented by law enforcement to obtain the search warrant is not the focus here, the majority's opening comments, written by Fish J., are now somewhat canonical in this area of law: "[i]t is difficult to imagine a search more intrusive, extensive, or invasive of one's privacy than the search and seizure of a personal computer."[661] This first SCC decision in the digital age did not drastically change the existing law,[662] but nonetheless set the table for what was to come.

Two years after *Morelli*, the SCC examined whether Canadians could reasonably expect to keep private the contents of a computer provided by an employer in *R v Cole*.[663] This time, the notion of reasonable expectation of privacy was examined in more depth by the Court, following the four step "totality of circumstances" test previously set forth in *Tessling*.[664] On the first factor, when it comes to the identification of the subject matter of the case, the Court specified that in such case, it is the informational content of the computer that is to be considered, not the physical device itself.[665] Since this decision, it has become clear that this will usually be the case (except possibly in circumstances where the device itself is being seized for an offence such as theft). The second and third factors were also fairly straightforward, as the accused's use of the computer to access the internet and store personal information showed that he had a direct interest in the contents of the computer and a subjective expectation of privacy towards them.[666] The main question was whether this

[661] *Ibid* at para 2.
[662] Aylward, *supra* note 655 at para 10.
[663] *Cole*, *supra* note 30.
[664] *Ibid* at para 40; *Tessling*, *supra* note 250 at para 32.
[665] *Cole*, *supra* note 30 at para 41.
[666] *Ibid* at para 43.

subjective expectation of privacy was reasonable, considering the totality of the circumstances.

A computer, especially when able to connect to the Internet, can contain highly sensitive information that pertains to an individual's "biographical core of personal information," regardless of whom owns it.[667] The fact that the device was provided by the accused's employer was therefore only one of the relevant circumstances to consider. Similarly, the fact that the employer had strict policies in place concerning the personal use of the device was relevant, but not determinative. All things considered, the Court decided that the accused in this case had a reasonable expectation of privacy in the device, due to the specific usage he made of it.[668] Because the computer had been seized without a valid court authorization, its seizure was presumed unreasonable and contrary to s. 8 of the *Charter*. The prosecution was unable to rebut this presumption by invoking the principles relating to consensual searches, as the consent was not given by the rights holder (i.e., the accused), but by the employer.[669]

One short year after *Cole*, the SCC had the opportunity to write its most forward-looking decision yet when it comes to digital privacy, broadly conceived. In *R v Vu*,[670] Cromwell J. adopted a progressive vision of search and seizure law that recognized the unique characteristics of computers, which consequently allowed him to put aside traditional search and seizure rules in favor of a new framework. *Vu* is aligned with a "technological novelty" approach as it recognizes that computers (and other similar devices) are fundamentally

[667] *Ibid* at paras 47–48.
[668] *Ibid* at para 58.
[669] *Ibid* at paras 77–78. See also *Reeves*, *supra* note 250 and Section 5.3.2 *infra*.
[670] *Vu*, *supra* note 1.

different from their "real-world" counterparts, such as filing cabinets or cupboards.[671] By refusing to resort to these simple comparisons, the SCC unanimously concluded that computers were distinct from other "receptacles" in at least four ways:

> First, computers store immense amounts of information, some of which, in the case of personal computers, will touch the "biographical core of personal information" referred to by this Court in *R. v. Plant*, [1993] 3 S.C.R. 281, at p. 293. […]
>
> Second, … computers contain information that is automatically generated, often unbeknownst to the user. […]
>
> Third, and related to this second point, a computer retains files and data even after users think that they have destroyed them. […]
>
> Fourth, limiting the location of a search to "a building, receptacle or place" (s. 487(1) of the *Code*) is not a meaningful limitation with respect to computer searches. […][672]

For these reasons, and because prior judicial authorization is "a cornerstone of our search and seizure law,"[673] the SCC decided that a warrant must explicitly provide for the search and seizure of devices and that it cannot be presumed that an issuing justice has considered the unique privacy interests in electronic data.[674] Accordingly, if the warrant is silent on this matter, law enforcement will only be allowed to seize the device to ensure the integrity of the data and will need to obtain another warrant before examining the contents of the device.[675]

---

[671] *Ibid* at paras 1–2.
[672] *Ibid* at paras 41–44.
[673] *Ibid* at para 46.
[674] *Ibid* at paras 46–47.
[675] *Ibid* at para 49.

The SCC's adoption of a "technological novelty" approach in *Vu* also meant the recognition that cellphones are now the equivalent of computers, due to their present-day capacities.[676] Following this comment made by Cromwell J. in *Vu*, one could have expected cellphones to receive a broad protection against warrantless intrusions by the state. However, and perhaps quite surprisingly, this was not the approach that was taken by the SCC in *Fearon*, a decision rendered only one short year after *Vu*. In *Fearon*, the SCC was divided 4 against 3 on the issue of whether law enforcement should be allowed to examine the contents of cellular devices without a warrant, incident to a lawful arrest.[677] The majority (written by Cromwell J.) concluded that the search incident to arrest doctrine could indeed allow for the warrantless search of cellphones, with only small modifications made to the conditions that need to be respected by law enforcement.[678] As mentioned by Aylward, this approach "contrasts starkly with the technological novelty orientation of the dissent"[679] (written by Karakatsanis J.) and also generally with the previous SCC digital era decisions.

In *Fearon*, the majority concluded that while cellphone searches may constitute a significant intrusion of privacy in specific cases, it will not always be the case if the search is kept at a minimum.[680] Essentially, the majority concluded that law enforcement's objectives in proceeding with such searches were more important than the individual right to privacy—which is reduced in case of lawful arrest[681]—and that these opposed interests could be adequately balanced if additional conditions were imposed on law enforcement.[682] *A*

---

[676] *Ibid* at para 38.
[677] *Fearon*, *supra* note 1 at para 1.
[678] See section 5.3.2 (A) *infra* for more detail on the applicable conditions.
[679] Aylward, *supra* note 655 at para 77.
[680] *Fearon*, *supra* note 1 at para 54.
[681] *Ibid* at para 56, referring to *R v Beare*, [1988] 2 SCR 387 at 413 [*Beare*].
[682] *Ibid* at para 74.

contrario, the dissenting judges would have allowed the warrantless search of cellphone incident to arrest only when exigent circumstances are present, due to the high privacy interests at stake.[683]

The situation at play in *R v Marakah*[684] was somewhat different from the cases considered so far, as it involved the seizure of an accomplice's cellphone and the search of its contents to find incriminating text messages. The main issue to be determined by the SCC thus was whether "Canadians [can] ever reasonably expect the text messages they send to remain private, even after the messages have reached their destination."[685] To answer this question, the Court once again used the "totality of the circumstances" test.[686]

On the first factor, the majority found that subject matter of the search was the electronic conversation between the two accomplices, which was the subject of the police's interest, and not the cellphone itself.[687] Qualifying the subject matter of the search as the electronic conversations properly reflected law enforcement's objectives, while considering "the technological reality of text messaging:"[688]

> When a text message is searched, it is not the copy of the message stored on the sender's device, the copy stored on a service provider's server, or the copy in the recipient's "inbox" that the police are really after; it is the electronic conversation between two or more people that law enforcement seeks to access.[689]

---

[683] *Ibid* at para 137-138 [Karakatsanis J.'s dissenting motives].
[684] *Marakah*, *supra* note 260.
[685] *Ibid* at para 1.
[686] *Ibid* at para 11.
[687] *Ibid* at paras 16–17.
[688] *Ibid* at para 17.
[689] *Ibid* at para 19.

As previously mentioned, properly qualifying the subject matter of the search will not always be easy, especially when it comes to electronic data.[690] However, it is crucial that courts remain cognizant of the fact that technological considerations should not be used to unduly limit s. 8's reach by adopting a narrow view of what the subject matter of the search really is.

As the author of the text messages found on the accomplice's phone, the accused had no issue proving he had a direct interest in the subject matter, following the second factor of the "totality of circumstances" test. Similarly, his subjective expectation of privacy was rather obvious. As it is often the case, the real issue was to determine if this subjective expectation of privacy was objectively reasonable. In the end, even if the accused did not have control over the device, the majority found that the accused's claims were indeed reasonable, mostly because electronic conversations, by definition, are capable of revealing an important amount of personal information.[691] The risk that a party to an electronic conversation reveals it to authorities did not negate an otherwise reasonable expectation of privacy.[692] In the end, the search was found to be unreasonable, as the Crown had conceded that this would be the case if the accused's subjective expectation of privacy was deemed reasonable under s. 8.[693]

Aylward's analysis of the SCC's decisions in the digital era was published prior to the court's decision in *Marakah*.[694] Accordingly, he did not categorize this decision following the two approaches he suggests. However, it seems safe to say that the majority's decision in *Marakah* fits squarely into the "technological novelty" approach, for a few reasons. First, the

[690] *Spencer*, *supra* note 241 at para 23; *Marakah*, *supra* note 260 at para 14.
[691] *Marakah*, *supra* note 260 at para 37.
[692] *Ibid* at para 40.
[693] *Ibid* at para 56.
[694] Aylward, *supra* note 655 at para 87.

categorization of the subject matter of the search in *Marakah* is novel in itself and recognizes the unique nature of text messaging.[695] Second, by granting the accused the standing under s. 8 of the *Charter*, the majority specifically avoided "analogies to the analog world," which are often relied upon under the opposed "technological neutrality" approach.[696] Third, and perhaps most importantly, by applying the control factor to the electronic conversation (rather than to the text messages found on his accomplice's phone) the majority recognized one of the unique features of digital data: the possibility of data existing at two different locations at the same time, without it impacting the privacy right of the rights-holder.[697] As no court would deem an electronic conversation found in the accused's phone to be undeserving of the protection against unreasonable search and seizure granted by s. 8 of the *Charter*, the same conversation found on another device was found to be worthy of the same level of protection. This is "technological novelty" at its very best.[698]

A contrario, in his dissenting reasons, Moldaver J. accepted the Crown's argument that the accused lacked standing to challenge the search, which effectively adopted the "technological neutrality" approach described by Aylward. In doing so, the dissenting judges relied heavily on the *ratio decidendi* of *Edwards* and the idea that control is essential to establish the

[695] Both the majority and the dissenting judges determined the subject matter of the search to be the electronic conversation that occurred between the accused and his accomplice. See *Marakah*, *supra* note 260 at paras 17, 111-112. However, this definitely had a bigger impact in the majority's decision.
[696] Aylward, *supra* note 655 at para 6.
[697] *Marakah*, *supra* note 260 at paras 38-45.
[698] One minor caveat should be noted here. Chelsey Buggie states that *Marakah* is "equilibrium adjustment," following Orin S Kerr's terminology (see Kerr, *supra* note 656), which would put it in the "technological neutrality" category. See Chelsey Buggie, "Talking to Strangers: A Critical Analysis of the Supreme Court of Canada's Decision in *R v Mills*" (2021) 44:5 Man LJ 108 at para 35. However, regardless on the end result, the analysis of the majority in *Marakah* can still be properly categorized as being "technological novelty" because of the forward-looking approach to electronic communications it employs to arrive at the abovementioned result.

existence of a reasonable expectation of privacy over the subject matter of the search.[699] Multiple "analogies to the analog world" are also made, including contrasting the control exercised over text messages with the one an accused has over DNA evidence, diaries, or garbage that is placed on the side of the road.[700] The dissenting judges' reasons in *Marakah* are difficult to reconcile with the rest of the SCC's jurisprudence on digital evidence, especially with the fact that sharing information with a third party has been found not to be fatal to a s. 8 claim, including in the subsequent decision *Reeves*.

In *Reeves*, the SCC examined whether the consent of a spouse can allow a warrantless seizure of a device that is shared between both spouses.[701] The majority (and Moldaver J. in his dissenting reasons) concluded that the accused had a reasonable expectation of privacy towards the computer and the data it contains, even though he shared control over the device with his spouse.[702] Consequently, the seizure was found to be contrary to s. 8 of the *Charter* because the accused's consent had not been obtained by law enforcement prior to the seizure.[703] This is a fairly straight-forward application of *Cole*, when it comes to the seizure of a computer pursuant to the warrantless first party consent search doctrine.[704]

What is possibly more surprising with *Reeves* is Côté J.'s dissenting motives and the fact that she focused on the difference between the warrantless seizure of the computer and its subsequent search, which was done in this case after the police had obtained a search warrant

[699] *Ibid* at paras 107-108, 113.
[700] *Ibid* at para 116.
[701] *Reeves*, *supra* note 250 at para 7.
[702] *Ibid* at paras 38-39, 70.
[703] *Ibid* at paras 47, 70.
[704] *Cole*, *supra* note 30 at paras 77-78.

some four months later.[705] By qualifying the subject matter of the search as being the computer itself (not the data it contained), Côté J.'s dissenting reasons are in stark contrast with a "technological novelty" approach, as it fails to recognize why law enforcement seized the computer in the first place. While *Vu* explicitly recognizes the difference between the seizure of a device and its subsequent search, it does so in the specific context of search warrants where a judge has previously determined that law enforcement satisfies the conditions put forth in s. 487 of the *Criminal Code*.[706] Here, Côté J.'s reasons omit the fact that law enforcement seized the device without a warrant for the sole purpose of eventually accessing its contents, in a situation where they could not have obtained a s. 487 search warrant because they lacked the grounds to do so. Her reasoning would effectively give law enforcement the power to seize (not search) any device without a warrant, which is inconsistent with the established jurisprudence on s. 8 of the *Charter*.[707]

One year after *Reeves*, the SCC examined the legality of a very specific investigative technique in *Mills II*.[708] In this case, the police had conducted an online sting operation where a police officer pretended to be a 14-year-old girl, with the objective of catching online child predators.[709] The accused corresponded with the undercover officer on Facebook and Hotmail and eventually arranged to meet the "child" in person. He was then arrested and charged with luring a child via the internet (s. 172.1 of the *Criminal Code*). The operation was conducted without prior judicial authorization and the Crown relied on screen captures to introduce the

[705] *Ibid* at paras 123-124.
[706] *Vu*, *supra* note 1.
[707] See *inter alia Cole*, *supra* note 30 at para 41, where J. Fish wrote: "the subject matter of the alleged search is the data, or *informational content* of the laptop's hard drive, its mirror image, and the Internet file disks — not the devices themselves."
[708] *Mills II*, *supra* note 264.
[709] *Ibid* at para 2.

record of the communications at trial.[710] The issues at trial were whether the investigative technique had amounted to a search or seizure, under s. 8 of the *Charter*, and whether the use of the screen capture software amounted to an intercept under Part VI of the *Criminal Code*.

Of all the seven justices who were present for this case, only one concluded that the accused had a reasonable expectation of privacy towards the recording that was made of his conversations with the undercover police officer. Martin J. started her analysis by comparing the case at bar with the situation that was present in *Duarte*.[711] Considering that the technique under review was the digital equivalent of the type of surveillance that took place in *Duarte*, she concluded that the applicant was right in his factum to qualify this case as "*Duarte* for the digital age."[712] As *Duarte* made it clear that the state cannot make permanent recording of private communications absent prior judicial authorization,[713] Martin J. concluded that the fact that the communication had been conducted on a medium that automatically creates a recording should not be used to lessen the protection afforded by the *Charter* and make that recording available to the state without prior judicial authorization.[714] As such, she concluded it was reasonable for the accused to expect that the state would not acquire the records of his private communications with the undercover police officer absent a judicial authorization. In Martin J.'s own words:

> Unregulated state access to electronic private communications engages s. 8 of the *Charter* because contemporary electronic communications are analogous to the surreptitious electronic recordings that attracted a reasonable expectation of privacy

[710] *Ibid* at paras 2-3.
[711] *Ibid* at paras 82-85.
[712] *Ibid* at para 86.
[713] *Duarte*, *supra* note 607.
[714] *Mills II*, *supra* note 264 at paras 89-90.

> in *Duarte*. While electronic communications possess the characteristics of informality and immediacy that define oral conversations, they also possess the characteristics of permanence, evidentiary reliability, and transmissibility that define electronic recordings. They are a form of the "documented record" (*Duarte*, at p. 54, referring to *White*, at pp. 787-89) to which the state seeks access. Thus for the "freedom not to be compelled to share our confidences" (*Duarte*, at p. 53) to retain any meaning, state access to electronic recordings of our private communications requires regulation. It was, therefore, objectively reasonable for Mr. Mills to expect not to be subjected to warrantless state acquisition of permanent electronic recordings of his private communications. The state action in this case constituted a search within the meaning of s. 8 of the *Charter*.[715]

Further, Martin J. concluded that the use of the screen capture software "Snagit" constituted an intercept as defined by s. 183 of the *Criminal Code*, making the technique subject to the strict conditions found within Part VI. She found the technique to be an intercept following the interpretation of that term found in *Jones II*, due to the fact that the undercover police officer had made the screen captures in "real-time."[716] For her, the fact that "we are wiretapping ourselves,"[717] by using services such as Facebook or Hotmail, should not be used to negate our right to be protected against the state intruding upon our privacy.

The other six justices concluded that the subjective expectation of privacy of the accused was objectively unreasonable, although they did not necessarily agree with the method to use to reach this conclusion.[718] Brown J.—writing for himself, Abella and Gascon JJ.—determined that the fact that the accused had been communicating with a "child" who was a stranger to

---

[715] *Ibid* at para 91.
[716] *Jones II*, *supra* note 249.
[717] *Mills II*, *supra* note 264 at para 141.
[718] As mentioned by Buggie, *supra* note 698 at para 6, while *Mills II* is technically a unanimous decision went it comes to the admissibility of the evidence, it is far from unanimous "with respect to the principles in the case."

him was determinative and foreclosed the accused's claim that his subjective expectation of privacy was objectively reasonable.[719] For her part, Karakatsanis J. determined that the investigative technique under review was no different than when an undercover police officer talks with a suspect and that the fact that the conversation took place in written form (rather than orally) did not transform the nature of the communication.[720] In essence, she concluded that the subjective expectation of privacy of the accused was unreasonable considering that it is not reasonable to expect that messages will be kept private from their intended recipient (regardless of who that person really is).[721] Further, she concluded that the use of "Snagit" did not constitute an intercept, because "the permanent record of the conversation resulted from the medium through which Mr. Mills chose to communicate."[722] Finally, Moldaver J. found that the reasons provided by Karakatsanis and Brown JJ. were both sound in law and justified the dismissal of the case.[723]

Justice Martin's position is aligned with a "technological novelty" approach, as it recognizes that electronic communication platforms have fundamentally altered our relationship with privacy and that using these platforms is a "virtual prerequisite to participation in society."[724] Rather than focusing on the fact that the SCC "has long recognized that s. 8 does not prevent police from communicating with individuals in the course of an undercover investigation,"[725] Martin J. adopted a forward-looking approach that "seek[s] to recalibrate values and privacy

[719] *Mills II*, *supra* note 264 at para 22.
[720] *Ibid* at paras 43-45.
[721] *Ibid* at para 44.
[722] *Ibid* at para 55.
[723] *Ibid* at para 66.
[724] *Ibid* at para 96.
[725] *Ibid* at para 42 [as per Karakatsanis J.'s reasons].

and public safety to a new societal context."[726] Effectively, her position stresses the importance of preventing unregulated state surveillance of electronic communications, regardless of the technical characteristics of a specific communication: if the state is creating a permanent recording of a private communication, in whatever way, shape, or form, prior judicial authorization is required.[727] Her dissent has been said to be the most consistent with the previous jurisprudence on s. 8 of the *Charter*.[728]

On the other side, Karakatsanis J.'s position is rooted in a "technological neutrality" approach that maintains the analog world idea that undercover police officers can communicate with suspects without prior judicial authorization. This approach fails to consider the fact that electronic communication technologies that create permanent recordings of communication by design have not changed the normative expectation of individuals that the state cannot access or make a permanent recording of a private communication without a judicial authorization.[729] Further, and although the "technological neutrality" approach is usually characterized by a desire to maintain the balance between privacy and public safety that existed prior to the advent of a new technology,[730] both the majority's position and Karakatsanis' reasons "unduly shifts the balance of power to favour law enforcement."[731] Indeed, if the position adopted had been to maintain the *status quo* that existed prior to the

---

[726] Aylward, *supra* note 655 at para 7, describing the characteristics of the "technological novelty" approach. The application of Aylward's dichotomous terminology to *Mills II* is novel to this thesis, as the decision was rendered two years after the publication of his article.
[727] *Mills II*, *supra* note 264 at para 72.
[728] Buggie, *supra* note 698 at para 6; Steven Penney, "'To Catch a Predator': Reasonable Expectation of Privacy in R v Mills", (23 April 2019), online: *University of Alberta Faculty of Law* <https://ualbertalaw.typepad.com/faculty/2019/04/to-catch-a-predator-reasonable-expectations-of-privacy-in-r-v-mills.html>.
[729] *Mills II*, *supra* note 264 at para 101 [as per Martin J.'s reasons].
[730] Aylward, *supra* note 655 at para 6.
[731] Buggie, *supra* note 698 at para 4.

advent and proliferation of electronic communications, the end result would have been quite different. As such, *Mills* is not only an embodiment of "technological neutrality" but also an amplification of it, especially when it comes to Karakatsanis J.'s motives.[732]

Finally, on the subject of the existence of a reasonable expectation of privacy in digital devices, it should be noted that as per *Fearon* and *Vu*, the nature of the device (i.e., whether it is a computer, a smartphone, or another type of device that allows the user to carry out similar functions) should not affect the analysis.[733] As long as the device being sought-after contains data that relates to "the biographical core of personal information," its search or seizure will be protected, to some degree, by s. 8 of the Charter. This makes a large array of devices susceptible of protection under s. 8, such as intelligent watches and other similar fitness tracking devices, some types of pacemakers and other personal medical equipment that uses the internet to communicate information from the user to their medical staff, and other connected devices from the IoT.

---

[732] Leonid Sirota (who currently teaches in the United Kingdom but studied law at McGill University) states that all three sets of reasons in *Mills II* illustrate to some degree Kerr's "equilibrium-adjustment theory," as they all seek to restore or preserve the balance that existed between privacy and security. Leonid Sirota, "What was Equilibrium Like?" (31 May 2019), online: *Double Aspect* <https://doubleaspect.blog/2019/05/31/what-was-equilibrium-like/>. Perhaps this is true to some extent, even though they arrive to very different results. However, because Justice Martin's reasons recognize the unique nature of electronic communications, they should still be qualified as falling in the "technological novelty" approach, regardless of the end result.

[733] *Fearon*, *supra* note 1 at para 54; *Vu*, *supra* note 1 at para 38. One major caveat needs to be restated here. While the majority in *Fearon* mentioned that a cellphone is the equivalent of a computer, it did not grant the same level of protection to both types of devices by allowing the warrantless search of cellphones seized incident to arrest. Accordingly, the specific protection afforded by s. 8 of the *Charter* to a device might vary depending on its type and the moment where it is seized or searched. The nature of the device, however, should not prevent a s. 8 analysis altogether, if the device contains private data.

5.2.2 The Existence of a Reasonable Expectation of Privacy Towards Personal Delocalized Data

The same year as *Vu*, the SCC examined in *R v TELUS Communications Company* whether technological differences between service providers should modify an individual's reasonable expectation of privacy towards their private communications.[734] In this case, law enforcement officials were seeking to obtain text messages from TELUS, using a general warrant found under s. 487.01 of the *Criminal Code*, under the pretence that TELUS' unique method of saving text messages onto its servers for a certain period of time during the delivery process had made this investigative technique a search or seizure, rather than an interception of private communications. As such, the Crown argued that the "wiretapping" provisions in Part IV of the *Criminal Code* were inapplicable, as the police were not trying to *intercept* the communications but obtain them from the company's servers.[735]

Justice Moldaver, writing for the majority,[736] concluded that the technique used by law enforcement in this case was "substantively equivalent" to a Part VI intercept.[737] Accordingly, he concluded that s. 487.01 of the *Criminal Code* had not been respected, due to the fact that another provision provided for an authorization permitting the technique contemplated by law enforcement, hence contravening s. 487.01(1)(c) of the *Criminal Code*. Consequently, a Part VI authorization needed to be obtained by the authorities because they were seeking "the

[734] *TELUS*, *supra* note 249.
[735] *Ibid* at paras 2–3.
[736] Moldaver wrote for himself and Karakatsanis J. However, his reasons can be qualified as being the majority because they were accepted by Abella J. at para 20, effectively giving him the support of the majority.
[737] *TELUS*, *supra* note 249 at para 52.

delivery of *future* private communications on a *continual*, if not continuous, basis over a sustained period of time,"[738] which is minimally tantamount to an intercept.[739]

For her part, Justice Abella, writing for herself, LeBel and Fish JJ., found that "[t]echnical differences inherent in new technology should not determine the scope of protection afforded to private communications."[740] As such, she deemed the investigative method suggested by law enforcement to be an intercept (not just "substantively equivalent" to one) because law enforcement was seeking to obtain the continuous production of prospective text messages from TELUS.[741] Consequently, and in agreement with Moldaver J.'s reasons, she found that law enforcement could not use the general warrant as a way of avoiding the more stringent requirements found in Part IV, as these requirements are necessary to protect the unique privacy interests found in private communications and they cannot be skirted by resorting to the general warrant provision,[742] which furthermore has a strictly residual application.[743] In sum, *TELUS* successfully restated the general principle that privacy protections need to be normative rather than descriptive, and that technological considerations are not the only relevant factors to consider when determining what type of judicial authorization is applicable to the investigative technique suggested by law enforcement.[744]

---

[738] *Ibid* at para 67.
[739] *Ibid*.
[740] *Ibid* at para 5.
[741] *Ibid* at para 45.
[742] *Ibid* at para 27.
[743] *Ibid* at para 18.
[744] See Moldaver J.'s reasons at para 68 where he states that the technique used by law enforcement was indeed technically different what would normally occur under a Part VI authorization but that this fact was not determinative when it comes to the "identical privacy interests at stake."

Prior to the explosion of computer use in our society, the SCC had examined in different contexts whether individuals retained a reasonable expectation of privacy towards information that they had voluntarily shared with a third party.[745] As mentioned before, the SCC concluded that control is only one of the relevant factors to be considered in the determination of a reasonable expectation of privacy. In *R v Spencer*,[746] the SCC assessed whether subscriber information—i.e., data that allows to link a specific IP address with a specific customer—could be treated in the same manner.

The investigative technique used in *Spencer* is very important for law enforcement. It allows them to link a specific usage of internet with a specific individual, more often than not in the context of child pornography. By conducting online surveillance of various sites or peer-to-peer sharing networks, specialized police officers will obtain the IP addresses of devices that were used in relation with the illegal content (either to upload or download the content). The next step is to identify the individual behind the device, which can be done by obtaining the subscriber information linked to that IP address from the responsible internet service provider (ISP).[747] In *Spencer*, law enforcement officials had obtained this information from the ISP without prior judicial authorization.[748]

Once again applying the "totality of circumstances" test, the Court unanimously concluded that the accused had a reasonable expectation of privacy in the subject matter of the search, which was identified as being not only the name and address of the person in a contractual

[745] See for example, *Gomboc*, *supra* note 291; *Colarusso*, *supra* note 567; *R v Dersch*, *supra* note 645.
[746] *Spencer*, *supra* note 241.
[747] *Ibid* at paras 7–11. This technique is widely used by law enforcement and multiple lower court decisions illustrate the same method. See *inter alia R v Pelich*, 2012 ONSC 3611; *R v Burke*, 2013 ONCA 424; *R v Owen*, 2017 ONCJ 729; *R v El-Halfawi*, 2021 ONCJ 462.
[748] *Spencer*, *supra* note 241 at para 11.

relationship with the ISP, but rather "the identity of an Internet subscriber which corresponded to a particular Internet usage."[749] To reach this conclusion, the Court specified that the inferences that can be drawn from personal internet usage information must be considered to properly identify the subject matter of the search, as otherwise it might be conceived too narrowly and would not reflect the privacy interests being invaded by the investigative technique.[750]

The Court also treated *Spencer* as an opportunity to specify what privacy actually means in the context of online communications. Previously, the SCC had mostly interpreted informational privacy through the lens of "confidentiality and control of the use of intimate information about oneself."[751] In the online context, however, the Court broadened its vision of privacy to include anonymity as one of the relevant factors to be considered. Anonymity is not restricted to online activities, as there are multiple situations where people communicate information only because of the promise that their identity will remain private.[752] Yet, because internet users are not in a position to fully control the traces they leave online, anonymity is even more important when using this medium, since it can be a tool to ensure that online activities remain private.[753] Anonymity is linked with the aspect of privacy that promotes individual growth and liberty of expression.[754]

As the subjective expectation of privacy of the accused was found to be reasonable, the warrantless seizure of the subscriber information was presumed unreasonable. In this case,

[749] *Ibid* at para 32.
[750] *Ibid* at para 31.
[751] *Ibid* at para 34.
[752] *Ibid* at para 42.
[753] *Ibid* at para 46.
[754] *Ibid* at para 48.

the prosecution was unable to rebut the presumption, as neither the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) or s. 487.014(1) of the *Criminal Code* create a police search and seizure power.[755] Consequently, law enforcement needed to obtain a production order to legally obtain the information from the ISP.

In *Jones II*,[756] the SCC examined whether historical text messages, i.e., text messages that have arrived at their destination and are not intercepted in transit, could be the subject of a reasonable expectation of privacy when obtained with a production order served on an accomplice's telecommunications service provider. Once again, the telecommunications service provider was TELUS and the obtention of the text messages was made possible because of the unique method that this company uses in the transmission process. Applying the "totality of the circumstances" test, the SCC unanimously found that the accused indeed had a reasonable expectation of privacy in the subject matter of the search, which was the electronic conversation that occurred between the accused and the co-accused.[757] However, the Court was divided as to the type of judicial authorization required to obtain historical text messages from a service provider.

The majority qualified the investigative technique used by law enforcement in this case as a simple seizure, rather than an interception of private communications, because it was not used to obtain "the *prospective* production of *future* text messages"[758] or messages still in the communication process but rather the production of *historical* text messages.[759] Accordingly,

[755] *Ibid* at para 71.
[756] *Jones II*, *supra* note 249.
[757] *Ibid* at para 9.
[758] *Ibid* at para 81.
[759] *Ibid* at paras 57, 59.

the majority found that a production order could validly be used to obtain *historical* text messages. This approach can be categorized as falling under the "technological neutrality" approach, as it keeps the traditional distinction between what constitutes an intercept and what does not, pursuant to the timing of the state's request in relationship to the transmission of the communication.

In dissent, Justice Abella adopted a "technological novelty" approach and contended that the timing of law enforcement's data acquisition should not modify the privacy protection afforded by the *Charter*.[760] She stressed that individuals should not receive lesser protection because of the service provider they choose to use.[761] Accordingly, she would have sided with the accused and decided that a Part VI authorization was necessary to obtain the messages from TELUS.[762] Justice Rowe, while in agreement with the majority on the applicability of a production order to obtain *historical* text messages, was also cognizant of the odd temporal distinction between a message that has just been sent and received, as opposed to one that is still in the communication process; a mere moment can dictate the level of protection a communication receives.[763]

Finally, it is important to note that Canadians cannot reasonably expect *all* their online activities to remain private. As noted previously, the majority in *Mills II*[764] found that "adults cannot reasonable expect privacy online with children they do not know."[765] Accordingly, no prior judicial authorization is necessary for law enforcement to conduct sting operations

[760] *Ibid* at para 93.
[761] *Ibid*.
[762] *Ibid*.
[763] *Ibid* at paras 83-87.
[764] *Mills II*, *supra* note 264.
[765] *Ibid* at para 23.

online and to use screen captures of the conversations at trial, to prove the accused's guilt for the offense of child luring.[766]

5.3 The Lawful Authorizations Applicable to the Search or Seizure of Digital Devices and Electronic Data

Examining the various authorizations found in the *Criminal Code* and warrantless powers stemming from the common law is necessary to determine whether existing powers can allow for the compelled unlocking of devices or decrypting of data. For this reason, this section will examine these provisions and common law powers and focus on their application in relation to electronic evidence or devices.

This will set the table for Part 2 of this thesis, which will demonstrate that neither the *Criminal Code* nor the common law currently provides law enforcement with power to compel individuals to decrypt or unlock their devices.

5.3.1 The Authorizations Found in the Criminal Code

In *Hunter*, the SCC found that the issuance of a judicial authorization prior to a search or seizure was an important requirement under common law and under s. 8 of the *Charter*. This requirement allows the courts to properly balance the privacy interests of the individual with the interests of the state.[767] Further, it serves as a safeguard against potential abuses of power

[766] It is worth mentioning at this point that *Mills II* has not been well received by commentators, including due to the fact that it does not follow well established jurisprudence on content neutrality. See *inter alia* Buggie, *supra* note 698; Lisa Silver, "A Look Down the Road Taken by the Supreme Court of Canada in *R v Mills*", (8 May 2019), online: *University of Calgary Faculty of Law* <https://ablawg.ca/2019/05/08/a-look-down-the-road-taken-by-the-supreme-court-of-canada-in-r-v-mills/>; Penney, *supra* note 728.
[767] *Hunter*, *supra* note 31 at 160.

by the state, as it verifies that law enforcement satisfies the specific conditions applicable to the issuance of the relevant authorization.

A) The Search Warrant (s. 487 of the Criminal Code)

The search warrant provided for by s. 487 of the *Criminal Code* will be the applicable authorization in most cases where law enforcement seeks to access the contents of a device found in a specific location, such as a home or a workplace.[768] Its issuance depends on the presence of reasonable grounds to believe that:

> there is in a building, receptacle or place
>
> > (a) anything on or in respect of which any offence against this Act or any other Act of Parliament has been or is suspected to have been committed,
> >
> > (b) anything that there are reasonable grounds to believe will afford evidence with respect to the commission of an offence, or will reveal the whereabouts of a person who is believed to have committed an offence, against this Act or any other Act of Parliament,
> >
> > (c) anything that there are reasonable grounds to believe is intended to be used for the purpose of committing any offence against the person for which a person may be arrested without warrant, or
> >
> > (c.1) any offence-related property.[769]

As mentioned, the warrant will need to specifically authorize the seizure and subsequent search of the devices found in a location. This ensures that the issuing judge has properly considered the high privacy interests present in electronic devices.[770] However, a new warrant

[768] *Morelli*, *supra* note 30; *Cole*, *supra* note 30.
[769] *Criminal Code*, *supra* note 37, s 487.
[770] *Vu*, *supra* note 1 at paras 46–47.

will not be necessary "to overcome levels of security, encryption, fragmentation, password protection of deletion in relation to the information the [device] contain[s]."[771]

The issuing judge however will not necessarily need to impose "*ex ante* conditions" or "search protocols" to law enforcement, to regulate the manner in which the search of the devices will be conducted. The SCC in *Vu* concluded that these were not necessary first, because the manner in which a search is conducted is usually reviewed after the fact; and second, because it is difficult to predict in advance where in the device the relevant evidence will be found and what specific technique the officer in charge of the search will need to use in order to find it.[772] The issuing judge will have the discretion to impose such conditions if the specific facts of the case require it, for example in instances where the search of the device might reveal confidential intellectual property, privileged information, or negatively impact third parties' privacy rights.[773]

Regardless of the presence of a search protocol, law enforcement will still need to conduct the search in a reasonable manner, as per the third prong of the *Collins* test. Effectively, this means that the scope of the search will need to be tailored to the specific evidence law enforcement is seeking in the device. In other words, the warrant does not give law

[771] *R v Twitchell*, 2010 ABQB 693 at para 32.
[772] *Vu*, *supra* note 1 at paras 53–59.
[773] *Ibid* at para 62. For example, in *United State v Equinix Inc*, 2017 ONCA 260, the Court determined that an independent party can be appointed to assist a judge in examining evidence collected pursuant to a search warrant to determine if it should be communicated to the authorities, under s. 15 of the *Mutual Legal Assistance in Criminal Matters Act,* RSC 1985, c 30 (4th supp). In this case, the warrant had authorized the seizure of computer servers which contained information that belonged to third parties and counsel for the appellant argued that this information should not be communicated to the American authorities. While not based on *Vu*, this is definitely a scenario where search protocols are useful to preserve third parties' privacy rights and strict conditions should be imposed by the issuing judge in the warrant.

enforcement "a licence to scour the devices indiscriminately."[774] For example, in *A c R*, a recent decision from the Quebec Superior Court, it was decided that the warrant was too ambiguous when it comes to the description of the sought-after evidence, which in turn lead to an unreasonable search.[775]

While seemingly obvious, compliance with the third prong of the *Collins* test has proven to be a difficult in practise. The search of a device can sometimes reveal evidence of new crimes, not listed in the previously obtained warrant. The question is then to determine if the discovery of the evidence of the new crime respects s. 8 of the *Charter*. *R v Jones*, from the Ontario Court of Appeals, appears to be accepted as the leading authority on the subject.[776] In this decision, the Court decided that in such situations, the first piece of evidence found will be admissible under the "plain view" doctrine but that a new warrant needs to be obtained in order for law enforcement to validly continue searching the device for evidence related to the newly discovered crime.[777]

Subsections (2.1) and (2.2) of s. 487 of the *Criminal Code* contain provisions specific to the execution of a search warrant on computers:

> Operation of computer system and copying equipment

[774] *Vu*, *supra* note 1 at para 61.
[775] *A c R*, 2021 QCCS 5440 at paras 159–160.
[776] *R v Jones*, 2011 ONCA 632, cited with approbation *inter alia* in: *R v KZ*, 2014 ABQB 235; *R v Johnson*, 2021 ONSC 1307; *R c Bissonnette*, 2020 QCCS 845 at para 9; *R v Kossick*, 2018 SKCA 55 at para 43; *R v Ferguson*, *supra* note 174.
[777] For a different perspective on this subject, see *Uber Canada inc c Agence du revenu du Québec*, 2016 QCCS 2158 at paras 281–284. In this tax related case, the Superior Court of Quebec mentioned *in obiter* that it will occasionally be necessary to search a device meticulously in its entirety, in order to find the relevant evidence. The Court recognized that this will inevitably sometimes lead to the discovery of unrelated evidence and possibly make the manner in which the search was conducted unreasonable. The only way of ensuring that the this will not be the case would then be to create a rule that makes this type of evidence inadmissible.

(2.1) A person authorized under this section to search a computer system in a building or place for data may

(a) use or cause to be used any computer system at the building or place to search any data contained in or available to the computer system;

(b) reproduce or cause to be reproduced any data in the form of a print-out or other intelligible output;

(c) seize the print-out or other output for examination or copying; and

(d) use or cause to be used any copying equipment at the place to make copies of the data.

Duty of person in possession or control

(2.2) Every person who is in possession or control of any building or place in respect of which a search is carried out under this section shall, on presentation of the warrant, permit the person carrying out the search

(a) to use or cause to be used any computer system at the building or place in order to search any data contained in or available to the computer system for data that the person is authorized by this section to search for;

(b) to obtain a hard copy of the data and to seize it; and

(c) to use or cause to be used any copying equipment at the place to make copies of the data.[778]

These provisions have been interpreted as simply giving law enforcement the right to access the devices and the data they contain, without involving any positive action from the owner or entity in control of the devices.[779] Further, s. 487(2.1)(a) of the *Code* has been interpreted as giving law enforcement access to any data that is accessible from the device, including data

[778] *Criminal Code*, *supra* note 37, s 487(2.1), (2.2).

[779] *R c Boudreau-Fontaine*, 2010 QCCA 1108 at para 46. This decision will be analyzed more thoroughly in Part 2 of this thesis.

that is found on a cloud,[780] which can be surprising considering they were adopted in 1997, a time where cloud computing was nowhere as pervasive as today.[781]

B) The General Warrant (s. 487.01 of the Criminal Code)

The general warrant provision was crafted in response to the SCC decision in *Wong*, to address concerns that law enforcement did not have sufficient powers to investigate crime.[782] Section 487.01 of the *Criminal Code* now allows law enforcement to use creative investigative techniques, including the type of video monitoring that took place in *Wong*.[783] Various types of investigative techniques have been allowed under this provision since its adoption, including:

- Conducting surreptitious video surveillance in locations where the individuals have a reasonable expectation of privacy;
- Simulating a break-in in order to seize drugs and money without having to notify the owners of the residence;[784]
- Taking a photograph of the accused's penis in order to identify him using a distinctive feature;[785]

[780] *R v Stack*, 2021 ONCJ 274.
[781] For territorial issues related inter alia to this provision, see Chapter 8, *infra*. See also Laura Ellyson, "La saisie de données situées dans le nuage en droit criminel canadien" (2019) 17:1 CJLT 1 at 23.
[782] *R v Kuitenen*, 2001 BCSC 677 at para 32.
[783] *R v Wong*, 2017 BCSC 306 at para 41.
[784] *R v Battista et al*, 2011 ONSC 4771 at para 67.
[785] *R v H-G (R)*, 2005 QCCA 1160.

- Conducting surreptitious entries into various locations, including cars,[786] storage units,[787] or "stash house[s]";[788]
- Seizing luggage at the airport and instructing the airline company to explain to the accused that the luggage was lost;[789]

And more specifically in relation with computers:

- Compelling a witness to assist law enforcement in recovering data using the recovery phone number listed by the accused that had been re-assigned to them;[790]
- Examining emails previously downloaded by law enforcement under a different authorization;[791]
- Examining data found in computers during a surreptitious entry into a commercial building.[792]

What these techniques have in common is that no other provision in the *Criminal Code* allows for their use. Indeed, as per the text of s. 487.01 of the *Criminal Code* and as interpreted by the SCC in *TELUS*, the general warrant provision is only applicable when no other provision would allow law enforcement to use the desired technique.[793] Further, a general warrant will be issued only when the police have reasonable grounds to believe that the use of the technique will provide information concerning the alleged offence and that the use of the technique is

[786] *R v Lucas*, [2009] CanLII 43423 (ON SC).
[787] *O'Reilly c R*, 2017 QCCA 1283.
[788] *R v Chen*, 2017 ONSC 4083.
[789] *R v Cody*, [2013] CanLII 94260 (NL SC).
[790] *R v Strong*, 2020 ONSC 7528.
[791] *R v Merritt*, 2017 ONSC 5245.
[792] *O'Reilly c R*, *supra* note 787 at para 94.
[793] *TELUS*, *supra* note 249 at para 20.

"in the best interests of the administration of justice."[794] In this context, the determination of what is in the best interests of the administration of justice includes considering the breadth and the period of validity of the authorization granted;[795] the existence of other authorizations allowing for the same technique;[796] the intrusiveness of the proposed technique as opposed to the nature of the investigation and the importance of the evidence;[797] and the sufficiency of the privacy safeguards put in place.[798]

In his 2020 book on criminal procedure, Steve Coughlan examines the positive and negative aspects of the general warrant provision.[799] He underlines that the existence of the provision allows for judicial scrutiny that would be inexistant if law enforcement officials could simply act on their own, which is beneficial.[800] However, while the provision was created "to fill gaps left by Parliament,"[801] the provision has not prevented more common law search powers to be created, which is quite contradictory and limits the potential beneficial impacts of s. 487.01 of the *Criminal Code*.[802] Coughlan also points out some harmful results emanating from the provision, due to the fact that it can allow nearly any type of investigative technique. More importantly, he submits that some investigative techniques are not the subject of specific provisions—and thus fall within the purview of s. 487.01—not because their use has not been contemplated by Parliament, but rather because Parliament made a deliberate decision not to

[794] *Criminal Code*, *supra* note 37, s 487.01(1)(b).
[795] *R v Lucas*, *supra* note 786 at paras 30–32.
[796] *Application for a General Warrant Pursuant to s 487.01 Cr. C. (Re)*, [2008] CanLII 85918 (QC CQ).
[797] *R v Strong*, *supra* note 790 at para 119.
[798] *R v Ha*, 2009 ONCA 340 at para 54.
[799] Steve Coughlan, *Criminal procedure*, fourth edition ed, Essentials of Canadian law (Toronto: Irwin Law, 2020)
[800] *Ibid* at 219.
[801] *Ibid*, referring to *Kang-Brown*, *supra* note 229.
[802] Coughlan, *supra* note 799 at 220.

authorize them.[803] This point is especially interesting when it comes to the regulation of investigative techniques that use new technologies via the general warrant provision.[804]

C) The Various Production Orders (ss. 487.014 and following of the Criminal Code)

Bill C-13, the *Protecting Canadians from Online Crime Act*,[805] which received royal assent in December 2014, radically overhauled the production orders available to law enforcement. According to the Honorable Peter MacKay, who was Minister of Justice at the time, these modifications to the *Criminal Code* were motivated in large part by the need to bring law enforcement "into the 21st century."[806] The various provisions were also a reaction to the SCC's decision in *Spencer*,[807] as well as being required for Canada to implement the Council of Europe's *Convention on Cybercrime*.[808]

Law enforcement now has access to a general production order (s. 487.014 of the *Criminal Code*) and a series of more specific orders: production order to trace specified communication (s. 487.015); production order – transmission data (s. 487.016); production order – tracking data (s. 487.017); and production order – financial data (s. 487.018). Additionally, two types of provisions now allow for the preservation of data, one directly by law enforcement with no prior judicial authorization (i.e., preservation demand, under s. 487.012) and one with prior

---

[803] *Ibid* at 222.

[804] As it will be submitted *infra* in Chapter 7, this thesis argues that the general warrant provision is ill-suited to regulate compelled decryption because of the unique self-incriminating nature of compelled decryption, which is not sufficiently addressed by s. 487.01 of the *Criminal Code*. This is also an argument for requiring Parliament to intervene to create a compelled decryption framework, rather than letting the courts do so.

[805] *Protecting Canadians from Online Crime Act*, SC 2014, c 31.

[806] Peter MacKay, "House of Commons Debates", (27 November 2013), online: <https://www.ourcommons.ca/Content/House/412/Debates/025/HAN025-E.PDF> at 1438.

[807] *Spencer*, *supra* note 241.

[808] Council of Europe, *Council of Europe Convention on Cybercrime* (ETS No 185), Budapest, 23 November 2001.

judicial authorization (i.e., preservation order, under s. 487.013). Apart from the general production order found in s. 487.014, which is subject to the *reasonable grounds to believe* standard, all these provisions can be used using the lower standard of *reasonable grounds to suspect*.[809] Production orders can only be used to obtain data that is the hands of a third party, usually a commercial entity, such as an ISP or TPDC.[810]

The Privacy Commissioner of Canada presented a submission to the Senate during the study of Bill C-13. In this submission, the Commissioner doubted the constitutional validity of the lower threshold of *reasonable grounds to suspect* that was suggested as being applicable to the new production orders, except to the general production order. The Commissioner was especially concerned about the possibility that seemingly innocuous data can be highly revealing when amalgamated and analyzed as a whole.[811] Accordingly, it was suggested that the higher threshold of *reasonable grounds to believe* should be made applicable to all the new production orders, or alternatively that the law enforcement should be barred from using that data in subsequent investigations or other purposes. Nonetheless, the new investigative powers were adopted without modification as to the applicable threshold. No specific limitation as to the subsequent use of data was included either.

---

[809] The lower standard applicable to s. 487.016 has been reviewed and determined to respect the Charter in *R v Otto*, 2019 ONSC 2473 at para 80 [*Otto*]. However, the Court left the door open for this question to be reconsidered in other scenarios where the use of the provision could reveal "core biographical information warranting a higher constitutional standard of protection.".

[810] See *Criminal Code*, *supra* note 37, ss. 487.014(4), 487.015(5), 487.016(4), 487.017(4), and 487.018(5).

[811] Daniel Therrien, "Bill C-13, the Protecting Canadians from Online Crime Act - Submission to the Standing Senate Committee on Legal and Constitutional Affairs", (19 November 2014), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2014/parl_sub_141119/>.

As such, the following table reflects what is currently applicable in Canada, when it comes to the new investigative techniques provided by Bill C-13. It provides examples of what type of data can be obtained (or protected) by law enforcement, and the applicable threshold.

Investigative Power	**Example of data *obtained***	**Threshold**
Preservation demand - 21 days (s. 487.012)	No data	suspicion
Preservation order – three months (s. 487.013)	No data	suspicion
General production order (s. 487.014)	Any stored data	belief
Production order to trace specified communication (s. 487.015)	Email, Internet Protocol (IP) and MAC addresses	suspicion
Production order – transmission data (s. 487.016)	IP addresses, website domains / pages visited, file sharing and other protocols, packet numbers, search engine search terms and email addresses	suspicion
Production order – tracking data (s. 487.017)	Location information, GPS coordinates	suspicion
Production order – financial data (s. 487.018)	Account holder information, types of accounts, date of account, current address	suspicion
Warrant for tracking device – transactions and things (s. 492.1(1))	Locations of credit or bank card usage, movements of vehicles	suspicion
Warrant for tracking device – individuals (s. 492.1(2))	Location of tracked individual (via personal mobile device)	belief
Warrant for transmission data recorder (s. 492.2)	See above	suspicion

Figure 3 Various Investigative Powers Found in the *Criminal Code* and their Applicable Threshold[812]

It is interesting to note that although Bill C-13 was adopted in part to address the fact that *Spencer* made it necessary for law enforcement to obtain an authorization before obtaining subscriber information from an ISP, no specific production order is applicable to obtain this information, with the lower threshold of *reasonable grounds to suspect*. Indeed, according to

[812] *Ibid*. It should be noted that the table includes information on preservation demands and orders, as well as specific types of warrants. These provisions are not discussed here due to their peripheral use when it comes to the encryption debate, although preservation demands and orders are definitely a useful tool that law enforcement can use to ensure data will be preserved until they can access it. The table was not altered, as to respect the original document's formatting.

the Provincial Court of Alberta, subscriber information can only be obtained with a general production order, which means law enforcement must respect the higher threshold of *reasonable grounds to believe*.[813]

D) The Collection of DNA and Fingerprints Samples

Following the SCC decision in *Borden*, the *Criminal Code* was modified to allow for the seizure of genetic material for the purposes of identifying individuals having committed a crime.[814] Section 487.05 of the *Criminal Code* now allows for the issuance of a warrant to take bodily substances for forensic DNA analysis, in order to compare a suspect's DNA material with a sample found during the course of the investigation of a designated offence.[815] In this context, the analysis of the genetic material is limited to the comparison between the suspect's sample and the previously obtained sample.[816]

The collection of DNA samples is also possible once an individual has been found guilty of a primary designated offence, under s. 487.051 of the *Criminal Code*. These offences can generally be described as being the more serious offences found in the *Code*, such as sexual offences towards children, murder, and terrorism offences. The purpose of this collection is to add the sample to the *National DNA Data Bank*, which was established by the *DNA Identification Act*.[817] In any case, whether under s. 487.05 during the course of an

[813] *Re Subscriber Information*, 2015 ABPC 178, cited with approbation in *Otto*, *supra* note 809 at para 15. See also Fehr, *supra* note 319 at 99, who cites other sources agreeing with this interpretation of the various production orders found in the *Criminal Code.*
[814] For an account of how that change came to be, see Neil Gerlach, *The genetic imaginary: DNA in the Canadian criminal justice system*, Digital futures (Toronto: University of Toronto Press, 2004), especially Chapter 3.
[815] The list of designated offences is found at *Criminal Code*, *supra* note 37, s 487.04.
[816] *SAB*, *supra* note 430 at para 13.
[817] *DNA Identification Act*, SC 1998, c 37.

investigation or s. 487.051 for convicted offenders, only specific methods of collection are authorized. These methods are relatively non-invasive, as they are limited to the plucking of hair, the taking of buccal swabs, and the taking of blood by pricking the skin surface.[818] Other methods of obtaining DNA samples are not available under the *Criminal Code*.[819]

When it comes to fingerprints, the *Identification of Criminals Act*,[820] allows for the taking of photographs and fingerprints of individuals charged of an indictable offence, which includes hybrid offences.[821] Some controversy exists as to the existence of a common law power to take fingerprints when an individual has been arrested but not yet charged of a crime. According to some courts, fingerprinting of someone arrested for an indictable offence is possible at common law,[822] while other courts concluded that the *Identification of Criminals Act* removed that power by making arrest a pre-condition to fingerprinting.[823] In any case, fingerprinting has been qualified as "minimally intrusive and has been recognized by statute and practise for such an extended period of time that [the SCC] readily found that it was acceptable in Canadian society."[824]

What is more important for our purposes than determining which legal current should be followed is that all of these decisions are concerned with the taking of fingerprints for comparison purposes only. Indeed, whether under the *Identification of Criminals Act* or a possible common law power, fingerprinting is done to compare two sets of prints; to

---

[818] *Criminal Code*, *supra* note 37, s 487.06.
[819] *Saeed*, *supra* note 583 at para 148.
[820] *Identification of Criminals Act*, RSC 1985, c I-1.
[821] *Interpretation Act*, RSC 1985, C I-21, s 34.
[822] *R v Pelucco*, 2013 BCSC 588; *R v Nguyen*, 2013 BCSC 950; *R v Bishop*, 2013 BCSC 522; *R v Do*, 2002 BCSC 1889.
[823] *R v Connors*, [1998] CanLII 12468 (BC CA); *R v Nicholson*, [1999] CanLII 6728 (NS SC).
[824] *Stillman*, *supra* note 353 at para 90.

determine if there is a match capable of proving that a suspect touched an object for example. Similarly, when it comes to photographing a suspect or someone charged with a crime, the photograph is only used for identification purposes. None of these decisions analyzed fingerprinting (or photographing) in the context of an investigative technique capable of giving law enforcement access to more than the inferences that can be drawn from a positive match between two samples, such as unlocking a device protected by a biometric authentication measure.

5.3.2 The Different Warrantless Search and Seizure Powers Available to Law Enforcement

A warrantless search or seizure is presumed to be unreasonable and the party seeking to justify such a warrantless search will have to rebut this presumption of unreasonableness.[825] Since this principle was established in *Hunter*, the courts have allowed for different types of warrantless searches or seizures, including under the doctrine of search incident to arrest, in the presence of exigent circumstances, or when the rights holder consents to the search. Because of their application when it comes to digital devices and evidence, these three types of warrantless searches will be further examined in this section. It should be noted however that other types of warrantless searches or seizures—including under the plain view doctrine that was referred to *supra*—exist either at common law or under statutory sources.

A) Search Incident to Arrest

Rooted in the evolution of the common law in England, the power of search incident to arrest has been long recognized by Canadian criminal law. It allows law enforcement to conduct a

[825] *Hunter*, *supra* note 31 at 161.

"frisk" search, in furtherance of a valid objective linked to criminal justice, usually to safeguard the safety of the police, the accused, or the public, or to discover evidence.[826] This power is truly exceptional, as it allows for a warrantless search, in a situation where law enforcement does not need reasonable and probable grounds prior to conducting it.[827] This extraordinary power is justified by the need to equip law enforcement with adequate powers,[828] in situations where less intrusive alternatives do not exist.[829]

In a context not involving electronic devices, three conditions must be respected by law enforcement in order for the search incident to arrest to be valid: "(1) the person searched is lawfully arrested; (2) the search is "truly incidental" to arrest, i.e., for a valid law enforcement purpose related to the reasons for the arrest; and (3) the search is conducted reasonably."[830] In *Fearon*,[831] the SCC examined whether these three conditions were sufficient to properly safeguard the unique privacy interests arising from the search of cell phone incident to arrest. Ultimately, the majority found that the search of electronic devices incident to arrest was necessary as to not unduly impede criminal investigations but that the conditions needed to be slightly modified to better reflect the unique nature of the data found on devices.[832]

Accordingly, a search incident to arrest of an electronic device will need to respect the following conditions:

---

[826] *Cloutier v Langlois*, *supra* note 620 at 186.
[827] *Fearon*, *supra* note 1 at para 16.
[828] *Beare*, *supra* note 681; *Debot*, *supra* note 646 at 1146; *Caslake*, *supra* note 617 at para 17.
[829] *Cloutier v Langlois*, *supra* note 620 at 185.
[830] *R v Tim*, 2022 SCC 12 at para 49 (references from original omitted).
[831] *Fearon*, *supra* note 1.
[832] *Ibid* at paras 63, 74.

(1) The arrest was lawful;

(2) The search is truly incidental to the arrest in that the police have a reason based on a valid law enforcement purpose to conduct the search, and that reason is objectively reasonable. The valid law enforcement purposes in this context are:

(a) Protecting the police, the accused, or the public;

(b) Preserving evidence; or

(c) Discovering evidence, including locating additional suspects, in situations in which the investigation will be stymied or significantly hampered absent the ability to promptly search the cell phone incident to arrest;

(3) The nature and the extent of the search are tailored to the purpose of the search; and

(4) The police take detailed notes of what they have examined on the device and how it was searched.[833]

In reaching this conclusion, Cromwell J. for the majority rejected the idea that search incident to arrest of electronic devices should only be allowed in the presence of exigent circumstances. He noted that this approach did not properly balance the opposed interests at play by giving "almost no weight to the law enforcement objectives served by the ability to promptly search a cell phone incidental to a lawful arrest."[834] The timing consideration thus seems to have been an important preoccupation of the Court in reaching its decision.

[833] *Ibid* at para 83.
[834] *Ibid* at para 70.

The majority did not discuss the impact that password and encryption can have on the search of devices incident to arrest.[835] Karakatsanis J., in her dissent, briefly mentioned the situation where a password can impede the search of a device but her comments are of a very general nature and do not provide much guidance when it comes to the possibility of compelling a suspect to unlock a device.[836] However, this *obiter* is interesting for at least three reasons: (1) it recognizes that the Court did not receive sufficient evidence on these questions;[837] (2) it implicitly admits that the majority's scheme only applies when no password or encryption is activated on the device; and (3) it suggests that a password-protected device that is unlocked at the time of the arrest may provide law enforcement with the power to enter the device to disable the password protection, under the doctrine of exigent circumstances.

B) Exigent Circumstances (s. 487.11 of the Criminal Code)

The presence of exigent circumstances can justify an otherwise illegal search or seizure.[838] Section 487.11 of the *Criminal Conde* explicitly recognizes that the presence of such circumstances can justify a warrantless search or seizure, in situations where the time necessary for law enforcement to fulfill the usual conditions for judicial authorization would seriously undermine the objectives pursued by the police. This provision was adopted following the SCC decision in *R v Silveira*.[839] As per *Grant*, exigent circumstances are present

[835] The majority only mentioned that the presence or absence of a password should bear little weight in the determination of a reasonable expectation of privacy towards the device. *Ibid* at para 53.
[836] *Ibid* at para 148.
[837] This is not surprising considering that the accused's cellphone was not password-protected. However, keeping in mind that cellphone passwords were already widely used in the 2010s, it exemplifies the limitations of the adversarial justice system and the fact that some issues are better left to be determined by Parliament than by the courts. On the advantages of legislative action as opposed to judicial action, see also Section 7.3 *infra*.
[838] *Tessling*, *supra* note 250 at para 33; *Kang-Brown*, *supra* note 229 at para 13.
[839] *R v Silveira*, *supra* note 234. See *R v Lucas*, *supra* note 786 at para 14.

when there is "an imminent danger of the loss, removal, destruction or disappearance of the evidence sought… if the search or seizure is delayed in order to obtain a warrant."[840] While s. 487.11 gives law enforcement the possibility to skirt the warrant requirement, it does not however lower the prerequisites for conducting the search or seizure.

Specifically, when it comes to electronic devices, at least two decisions have suggested that the exigent circumstances doctrine can allow for the seizure—but not the search—of devices brought to a store to be repaired. In *R v Winchester* and *R v Villaroman*, both the Ontario Superior Court of Justice and the Court of Queen's Bench of Alberta recognized that law enforcement could seize a device without a warrant when a person having been charged by the owner of the device to repair it comes across illegal material (in both cases child pornography) and calls the police.[841] The exigent circumstances are twofold: (1) leaving the repairperson in possession of the computer puts them in possession of the illegal material; and (2) the store has no authority to refuse to give the device back to its owner if they decide to come back and retrieve the device, effectively leading to the loss of the evidence.[842]

In *R v Hart*,[843] the Ontario Court of Justice reached a similar conclusion as Karakatsanis J. did in her *Fearon* dissent. In this decision, the wife of the accused had called the police after discovering child pornography on the accused's computer, which was located in the basement of their home. Once arrived at the location, the police decided to seize the computer and copy the material on a storage device without a warrant, in light of the fact that the evidence was in a decrypted state at the time and that the device was usually password-protected and

[840] *R v Grant*, [1993] 3 SCR 223 at 189.
[841] *R v Villaroman*, 2012 ABQB 630; *R v Winchester*, 2010 ONSC 652.
[842] *R v Villaroman*, *ibid* at paras 51–53; *R v Winchester*, *ibid* at para 13.
[843] *R v Hart*, 2015 ONCJ 831.

possibly had strong encryption software on it. The contents of the device were only searched after a warrant had been obtained, four months later.[844] The fact that the evidence could be encrypted at any moment, rendering it unintelligible for law enforcement, was found to be an exigent circumstance allowing for the warrantless seizure of the material.[845] In reaching this conclusion, the Court mentioned that the police would have respected the conditions to obtain a warrant under s. 487 of the *Criminal Code*, having seen the illegal content on the computer screen themselves.[846]

C) Consensual Searches (Waiver of s. 8 Rights)

A seizure under s. 8 is defined as "the taking of a thing from a person by a public authority without that person's consent."[847] Accordingly, if an individual consents to a search the protection against unreasonable search or seizure is not triggered and the warrantless search will be deemed to be reasonable under s. 8 of the *Charter*. Consensual searches can be an important tool for law enforcement when neither the common law nor the *Criminal Code* provide them with the power to use a specific investigative technique. For example, the only way for law enforcement to obtain blood samples from a person charged with an offence at the time *Borden* was written was to obtain that person's consent.[848]

To be valid, consent must be given freely and voluntarily. This means that the person consenting to the search (and waiving their s. 8 rights) must be informed of the possible consequences of acting in such way, including being made aware of the crime(s) for which

[844] *Ibid* at paras 13–15.
[845] *Ibid* at paras 25, 27.
[846] *Ibid* at para 28.
[847] *Dyment*, *supra* note 291 at 431.
[848] *R v Borden*, [1994] 3 SCR 145 at 159 [*Borden*].

they are arrested and investigated, and being given the right to consult with counsel.[849] Further, the consent will need to be given by the rights holder, which is the party that has a reasonable expectation of privacy in the subject matter of the search. When it comes to computers and other digital devices, this will usually mean that consent must be given by the individual to which the data saved on the device belongs, regardless of actual ownership of the device itself.[850] Further, a shared control or ownership over a device will not negate a reasonable expectation of privacy from all the individuals that have a reasonable expectation of privacy in the device.[851]

5.3.3 Current Legislative Framework Applicable to the Interception of Private Communications

The covert interception of private communication—a subcategory of electronic surveillance—is a particularly invasive investigative technique that raises unique privacy considerations.[852] As with other techniques that implicate the state infringing upon a reasonable expectation of privacy, intercepts are subject to s. 8 of the *Charter* and its protection against unreasonable search and seizure.[853] Intercepts are the subject of specific

[849] *Ibid.*
[850] *Cole*, *supra* note 30.
[851] *Reeves*, *supra* note 250.
[852] *Araujo*, *supra* note 642 at para 21; *Duarte*, *supra* note 607 at 44.
[853] As put by Robert W Hubbard, Peter M Brauti & Scott K Fenton, *Wiretapping and other electronic surveillance: law and procedure* (Toronto: Canada Law Book, Thomson Reuters Canada, 2022), s 1:13: "the conclusion that electronic surveillance constitutes a search and seizure for the purposes of s. 8 was so obvious that in *R v Finlay*, [1985] 23 SCC (3d) 48, the first Canadian appellate case to address the issue, the point was conceded."

provisions found in Part VI of the *Criminal Code*, which aim to balance the privacy interests of individuals with law enforcement's objective of investigating and prosecuting crimes.[854]

Intercepts can take multiple forms, from the installation of listening devices in private properties to the use of body packs equipped with microphones.[855] The method that is the most relevant for our purposes depends on interception by more technical means, usually with the assistance of a service provider, either of oral or written communications, including text messages[856] and emails.[857] This method is also often termed "wiretapping."[858] The use of wiretaps is said to be as old as the telephone itself,[859] although digital technologies have definitely modified its functioning and scope. The effects of wiretaps on privacy are quite obvious. As put by one author:

> [u]nlike normal search warrants which seize evidence in one location at one point in time, wiretaps record all incoming and outgoing information "like a huge vacuum cleaner, indiscriminately sucking in the relevant with the irrelevant without

---

[854] *In the Matter of a Reference Pursuant to Section 27(1) of the Judicature act, Chapter J-1 of the Revised Statutes of Alberta, 1980, as amended, referred by Order in Council (OC 84/83) of the Lieutenant Governor in Council dated the 2nd day of February, AD 1983, to the Court of Appeal of Alberta*, [1984] 2 SCR 697 at 702 [*Wiretap Reference*], referring to *R v Commisso*, [1983] 2 SCR 121 at 124–125.

[855] *Wiretap Reference*, *ibid* at 711.

[856] *TELUS*, *supra* note 249 at para 5.

[857] As per the *Interpretation Act*, *supra* note 821, s 35(1), a telecommunication "means the emission, transmission or reception of signs, signals, writing, images, sounds or intelligence of any nature by any wire, cable, radio, optical or other electromagnetic system, or by any similar technical system." As such, emails are included, if they are the subject of a reasonable expectation of privacy (which they are according to *R v Weir*, 2001 ABCA 181) and if they are intercepted, rather than obtained after they have reached their destination. See *infra* and Hubbard, Brauti & Fenton, *supra* note 853, s 6:28. Accordingly, stored emails do not require the use of a Part VI authorization in order for law enforcement to consult and seize them. See inter alia *R v Giles*, 2007 BCSC 1147; *R v Cuthill*, 2016 ABQB 60 at para 98.

[858] Nathan Forester, "Electronic Surveillance, Criminal Investigations, and the Erosion of Constitutional Rights in Canada: Regressive U-Turn of a Mere Bump in the Road towards Charter Justice?" (2010) 73:1 Sask L Rev 23 at 24.

[859] *Ibid* at 31 citing Robert W Cosman, "A Man's House Is His Castle-'Beep': A Civil Law Remedy for the Invasion of Privacy" (1971) 29 Fac L Rev 3 at 15.

> distinction" for [anywhere] between 60 and over 240 days. To put the effect on privacy in perspective, in one recent case, police intercepted 14,000 communications, of which 83 were deemed relevant and 16 were sought to be admitted as evidence at trial. This massive acquisition of information also violates the privacy of innocent third parties who associate with the target(s) of wiretaps.[860]

This section will explore succinctly the particularities of the Canadian provisions regulating the interception of private communications.[861] The application of these findings to the subject of encrypted communications (i.e., data in transit) will be done subsequently in Chapter 10. Jurisdictional issues linked to the use of wiretaps will also be addressed in Chapter 10.

The legislative framework applicable to the interception of private communications is examined here for two reasons. First, Part VI of the *Criminal Code* is a perfect example of the additional protections that must be put in place in order to respect s. 8 of the *Charter* when not only an individual has a reasonable expectation of privacy but also an *enhanced* expectation of privacy. As this thesis will claim that encryption creates an *enhanced* expectation of privacy,[862] the provisions found in Part VI will consequently be useful, as a starting point to the base-level requirements that will need to be respected by law enforcement if they wish to compel a suspect to unlock a device or otherwise decrypt data, in a manner that complies with s. 8 of the *Charter*. Second, the "going dark" issue requires different solution to be put in place pertaining to the type of data that is protected by encryption and that law enforcement is trying to obtain in a readable state. For data at rest, compelled

[860] Jim Cruess, "Cost of Admission: One Rubber Stamp - Evaluating the Significance of Investigative Necessity in Wiretap Authorizations after *R v Araujo*" (2013) 22 DJLS 59 at 61 (references omitted).
[861] For a more complete analysis, see *inter alia* Hubbard, Brauti & Fenton, *supra* note 853; David Watt, *Law of electronic surveillance in Canada*, Carswell's criminal law series (Toronto: Carswell, 1979-).
[862] See Chapter 7 *infra*.

decryption is an interesting solution, as it allows law enforcement to access decrypted data in plaintext rapidly and efficiently. For data in transit, compelled decryption is inapplicable as it does not give law enforcement a method to *intercept* communications in a decrypted thus readable state. Accordingly, it is important to distinguish the potential solutions to the "going dark" debate—provided in Parts 2 and 3 of this thesis—in accordance with the type of data law enforcement is trying to obtain and the method it is seeking to use (i.e., search and seizure of *data at rest*, as opposed to the interception of *data in transit*).

A) The Evolution of the Law of Electronic Surveillance in Canada

Prior to the 1970s, the use of electronic surveillance was largely unregulated in Canada.[863] In 1969, the Ouimet Committee report was published,[864] advocating for the creation of a "federal legislation controlling the use of wiretapping and electronic eavesdropping."[865] The Committee found that conversations where both parties had a reasonable belief that the conversations would not be the subject of acquisition by others by electronic, mechanical or other devices should be protected by federal statute.[866] This eventually led to the overhauling of the *Criminal Code* (and other federal laws) and the creation of Part IV.1 on invasions of privacy.[867]

[863] Hubbard, Brauti & Fenton, *supra* note 853, s 1:2.; *Wiretap Reference*, *supra* note 854 at 702. See also Anne Turner, "Wiretapping Smart Phones with Rotary-Dial Phones' Law: How Canada's Wiretap Law Is in Desperate Need of Updating" (2017) 40 Man LJ 249 at 252–254.
[864] *Towards Unity: Criminal Justice and Corrections*, by Roger Ouimet (Ottawa: Canadian Committee on Correction, 1969).
[865] *Ibid*, cited in Hubbard, Brauti & Fenton, *supra* note 853, s 1:2.
[866] Law Reform Commission of Canada, *Electronic surveillance*, Working paper - Law Reform Commission of Canada No. 47 (Ottawa: Law Reform Commission of Canada, 1984) at 2.
[867] Hubbard, Brauti & Fenton, *supra* note 853, s 1:2.

In *Duarte*,[868] the SCC had to examine the constitutional validity of "consent" surveillance, which is "electronic surveillance in which one of the parties to a conversation, usually an undercover police officer or a police informer, surreptitiously records it."[869] In this case, the recording was both of the audio and video of the inside of an apartment unit where an undercover police officer and a police informer were to meet with the accused and other people to discuss a cocaine transaction. Both the informer and the officer had previously consented to the interception of their conversations, pursuant to s. 178.11(2)(a) of the *Criminal Code* (as it then was).[870]

From the outset, the SCC cautioned that the term "consent" surveillance was a misleading way to describe this technique, as only one party to the conversation has to consent to the recording for it to transform from an unauthorized (thus criminal) to an authorized interception.[871] The Court then went on to analyze the constitutional validity of this technique and to determine whether "risk analysis"[872] theory was applicable in Canada. Pursuant to this theory that comes from the United States, the recording of a conversation done with the consent of one of the participants to that conversation is nothing more than an extension of that person's memory. As such, if a co-conversationalist has decided to reveal information to that person, the co-conversationalist needs to assume the risk that the conversation can be recorded and disclosed to the authorities.[873]

---

[868] *R v Wiggins*, [1990] 1 SCR 61 [*Wiggins*] is mostly to the same effect.
[869] *Duarte*, *supra* note 607 at 38.
[870] *Ibid* at 36.
[871] *Ibid* at 38.
[872] *Ibid* at 40.
[873] *Ibid*.

The consequence of accepting this theory would be that law enforcement can unilaterally decide to engage in this "consent" or "participant" surveillance, without obtaining a judicial authorization.[874] This is precisely what Parliament intended to prevent by adopting Part IV.1 of the *Criminal Code*.[875] There is a major distinction between accepting the risk that a co-conversationalist can disclose our words to the authorities and accepting that the state can make a permanent recording of these same words without judicial oversight.[876] Accordingly, the SCC concluded that this type of surveillance is no different from surveillance that is conducted without the consent of any of the parties to the conversation.[877] As put by Justice La Forest:

> I am unable to see any similarity between the risk that someone will listen to one's words with the intention of repeating them and the risk involved when someone listens to them while simultaneously making a permanent electronic record of them. These risks are of a different order of magnitude. The one risk may, in the context of law enforcement, be viewed as a reasonable invasion of privacy, the other unreasonable. They involve different risks to the individual and the body politic. In other words, the law recognizes that we inherently have to bear the risk of the "tattletale" but draws the line at concluding that we must also bear, as the price of choosing to speak to another human being, the risk of having a permanent electronic recording made of our words.[878]

For these reasons, the Court concluded that "consent" or "participant" surveillance without judicial authorization was not reasonable under s. 8 of the *Charter* and that "risk analysis" theory was inapplicable in Canada.

---

[874] *Ibid* at 42.
[875] *Ibid* at 44.
[876] *Ibid*.
[877] *Ibid* at 47.
[878] *Ibid* at 48.

Following the SCC decisions in *Duarte* and *R v Wiggins,* Part IV.1 of the *Criminal Code* was amended to become what is now Part VI.[879] Around the same time, the Law Reform Commission of Canada advocated for reform in light of concerns that Part IV.1 did little to actually protect privacy and that it gave rise to problems of interpretation.[880] As it now stands, Part VI of the *Criminal Code* contains the only provisions that allow for the interception of private communications, while the general warrant provision found in s. 487.01 can be used to allow for other electronic surveillance techniques that do not fall within Part VI's purview.[881]

As with the use of search warrants under s. 487 of the *Criminal Code* to search computers and other digital devices,[882] the *Criminal Code* does not prescribe a specific technological method that must be followed by law enforcement to enforce a wiretap authorization.[883] As such, the technical means used is a matter of law enforcement discretion, within the limits of what constitutes a reasonable search or seizure, in accordance with *Collins*.[884]

---

[879] See *R v Tse*, 2012 SCC 16, [2012] 1 SCR 531 at para 24 [*Tse*], referring to *Duarte*, *supra* note 607; *Wiggins*, *supra* note 868.

[880] Law Reform Commission of Canada, *supra* note 866 at 7–8.

[881] Sections 492.1 (use of a tracking device) and 492.2 (use of a transmission data recorder) are also provisions that fall within the general category of "electronic surveillance." See Hubbard, Brauti & Fenton, *supra* note 853, s 1.11.

[882] *Vu*, *supra* note 1 at paras 53–59. See also Section 5.3.1 *supra*.

[883] As put by the SCC in *Lyons*, *supra* note 383 at 664, Part VI:

> "is broad legislation embracing in these extensive provisions the use of a wide range of radio, telephone, optical and acoustical devices for listening to and recording private communications as broadly defined. It is not 'wiretapping' legislation, nor eavesdropping legislation, nor radio regulation. It is the regulation of all these things and 'any other device' that may be used to intercept intelligence reasonably expected by the originator not to be intercepted by anyone other than the intended recipient."

[884] *R v Collins*, *supra* note 31 at 278.

B) Overview of Part VI of the Criminal Code

Part VI of the *Criminal Code*, alike its precursor Part IV.1, has been said to strike the appropriate balance between "the right of individuals to be left alone and the right of the state to intrude on privacy in furtherance of its responsibilities for law enforcement,"[885] by creating a system of prior judicial authorization that must be followed to intercept private communications. In this context, a private communication is defined as:

> any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it.[886]

Following this definition, it is clear that any method of intercepting a private communication, will be a search or seizure under s. 8 of the *Charter*.[887] *A contrario*, if the communication is not carried out in such way as to prompt such expectation of privacy (for example, a conversation that is broadcasted publicly or a text conversation held in a public online forum), it will not receive the protection against unreasonable search or seizure and law enforcement will be able to obtain the contents of the communication as they see fit.[888]

---

[885] *Duarte*, *supra* note 607 at 45.
[886] *Criminal Code*, *supra* note 37, s 183.
[887] *Duarte*, *supra* note 607 at 42–43; *R v Thompson*, [1990] 2 SCR 1111 at 1136–1137; *Wiggins*, *supra* note 868.
[888] See *Marakah*, *supra* note 260, *Jones II*, *supra* note 249 and generally Section 5.2.2 *supra* on the reasonable expectation of privacy in digital data including communications.

Further, s. 183 of the *Criminal Code* defines the term 'intercept' to include "listen[ing] to, record[ing] or acquir[ing] a communication or acquir[ing] the substance, meaning or purport thereof."[889] Basically, what this non exhaustive definition aims to encompass is any means by which the state "interjects itself into the communication process in real-time through technological means."[890] Because the term 'intercept' implies the acquisition of the communication during the course of its transmission,[891] communications that have arrived at their destination and are 'seized' at that moment by law enforcement are not subject to the more stringent requirements found in Part VI of the *Criminal Code*.[892] In other words, Part VI is applicable for the purpose of "securing *prospective* authorization for the delivery of *future* private communications,"[893] while the general production order found in s. 487.014 is applicable to the acquisition of *historical* communications that are no longer in the transmission process.[894] However, the fact that a service provider temporarily stores a copy of a message in its transmission process should not be used by law enforcement as a means to avoid the application of Part VI.[895]

---

[889] *Criminal Code*, *supra* note 37, s 183.

[890] *Jones II*, *supra* note 249 at para 72. It should be noted here that the majority's position in *Jones II* (cited here) is consistent with Cromwell J.'s dissenting reasons in *TELUS*, not with the majority's position in that decision. In *TELUS*, the SCC unanimously determined that individuals have a reasonable expectation of privacy towards their text messages. The crux of the matter resided in the determination of the appropriate judicial authorization that could allow the police to access text messages stored on the company's server, as part of its delivery system. Cromwell J. (alongside McLachlin C.J.) argued that the investigative technique was not an intercept; Abella J. (alongside LeBel and Fish JJ.) argued that it was an intercept; Moldaver J. (alongside Karakatsanis J.) argued that it was the *equivalent* to an intercept. Further, while he wrote only for two justices, Moldaver J.'s position can be qualified as the majority, as his reasons were implicitly accepted by Abella J. Accordingly, by citing Cromwell J. here, the majority's position in *Jones II* (McLachlin C.J., and Moldaver, Karakatsanis, Gascon and Côté JJ., reasons also accepted by Rowe J.) is a departure from *TELUS*.

[891] *Ibid*.

[892] *Ibid*.

[893] *TELUS*, *supra* note 249 at para 67.

[894] *Jones II*, *supra* note 249 at para 59.

[895] *TELUS*, *supra* note 249 at para 67.

To respect s. 8 of the *Charter*, a wiretap authorization must respect the "particularly rigorous safeguards"[896] set out in Part VI of the *Criminal Code*, as these have been determined to respect the minimal requirements imposed by the SCC in *Hunter*.[897] Part VI of the *Criminal Code* also contains notice requirements that have been deemed necessary to provide transparency and sufficient check on police powers, in a context where law enforcement is conducting investigations that are highly intrusive in nature.[898] Both consensual and non-consensual interceptions[899] require law enforcement to present a detailed affidavit to the competent judge in order to receive an authorization to intercept private communications.[900] Specific information must also be included in the issued authorizations, including the names of the known targets and a description of the location where the interception will take place.[901]

i. Criminalization of Unauthorized Interceptions

Part VI of the *Criminal Code* functions largely on the fact that any unauthorized interception of a private conversation constitutes an offence, under ss. 184(1) and 184.5, barring the application of one of the exceptions found in s. 184(2). Telecommunication service providers are protected from committing these offences when they intercept communications in order to provide their services.[902]

---

[896] *Ibid* at para 4.
[897] *R v Garofoli*, [1990] 2 SCR 1421 at 1444–1445 [*Garofoli*] referring to *Hunter*, *supra* note 31 at 168; *Duarte*, *supra* note 607 at 45.
[898] *TELUS*, *supra* note 249 at para 30 referring to *Tse*, *supra* note 879.
[899] *Criminal Code*, *supra* note 37, s 184.2(2) and 185(1)(c) to (h).
[900] These specific requirements are not analyzed here due because irrelevant to the main goal of analyzing the impact of encryption to the wiretapping of private communications.
[901] *Ibid*, s 184.2(4) and 186(4).
[902] *Ibid*, s 182(2)(e); *Jones II*, *supra* note 249 at para 62.

It is worth mentioning that "consent" surveillance done without a judicial authorization—like what was done in *Duarte* and *Wiggins*—is protected as an exception to the commission of the offence of intercepting a private communication by s. 184(2)a) of the *Criminal Code*. As such, this conduct is not illegal *per se*.[903]

ii. Interceptions with Consent

As mentioned previously, the *Criminal Code* was modified in 1993, following *Duarte* and *Wiggins* to address the fact that the Court had ruled warrantless interception of private communications to be contrary to s. 8 of the *Charter*.[904] Since then, the expression "interception with consent" has taken a different meaning than in *Duarte*. Rather, s. 184.2 of the *Criminal Code* now uses this terminology to describe the situation where one party to the conversation has consented to the interception and where the issuance of a judicial authorization is being requested by law enforcement. In this case, the conditions applicable to the issuance of the authorization are less stringent than when no party to the conversation has given their consent, as the investigative necessity requirement that normally applies to wiretaps[905] does not apply. Further, the use of this provision is not limited to specific offences but is rather applicable to the investigation of any crime found in the *Criminal Code* or in another federal act. Section 184.3 is to the same effect but allows for the application to be presented by any means of telecommunication, in circumstances where it is impracticable for the applicant to appear physically before a judge.[906]

---

[903] Pierre Béliveau & Martin Vauclair, *Traité général de preuve et de procédure pénales* (Cowansville: Éditions Thémis ; Éditions Yvon Blais, 2013) at para 1185.
[904] *Tse*, *supra* note 879 at para 24.
[905] *Criminal Code*, *supra* note 37, s 186(1)b) see *infra*.
[906] *Ibid*, s 184.3(1).

A specific type of interception with consent is also applicable when the interception is done for the purpose of preventing bodily harm, under s. 184.1 of the *Code*.[907] This provision, alongside s. 184.4,[908] has a preventative nature, as opposed to the investigative purpose that is usually prevalent when it comes to wiretap authorizations. [909]

iii. Interceptions without Consent

As the SCC mentioned in *R v Tse*, the general provisions applicable to the interception of private communications are found within ss. 185 and 186 of the *Criminal Code*.[910] These provisions are of an investigative nature and will therefore be used to gather evidence against suspects. Section 185(1) of the *Code* deals with the entities that can present applications for authorizations to intercept private communications, while s. 185(2) presents the general information that needs to be included in the affidavit in support to the application. Interceptions without consent are only available for specific offences that have been deemed to be serious enough to justify such an infringement of a target's reasonable expectation of privacy.[911]

In order for a wiretap authorization to be issued, s. 186 of the *Criminal Code* states two requirements in addition to the general requirement that the issuing judge must be satisfied that "there are reasonable and probable grounds to believe that an offence has been, or is being, committed and that the authorization will afford evidence of that offence."[912] These

[907] *Ibid*, s 184.1. In this case, however, the admissibility of the intercepted communications is highly limited by s. 184.1(2).
[908] See Section 9.2.4. *infra.*
[909] *Tse*, *supra* note 879 at para 25.
[910] *Ibid* at para 22. See also *TELUS*, *supra* note 249 at para 27.
[911] For the list of offences, see *Criminal Code*, *supra* note 37, s 183.
[912] *Duarte*, *supra* note 607 at 45.

additional requirements adequately reflect the heightened privacy interests that come into play with wiretaps.[913] The first additional requirement is that the issuance of the wiretap authorization is in the best interest of the administration of justice. This is the same requirement that is found under s. 487.01(1)(b) of the *Code*.[914]

The second additional requirement is currently only found in this specific provision of the *Criminal Code*. Under the 'investigative necessity' requirement, a wiretap authorization will only be issued when the judge is satisfied that "other investigative procedures have been tried and have failed, other investigative procedures are unlikely to succeed or the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using only other investigative procedures."[915] The requirement does not mean that the government must have indeed tried all other investigative techniques; only that alternative methods are unlikely to succeed in the circumstances.[916] The investigative necessity requirement finds its origins in England[917] and has also been imported into the American legislation on electronic surveillance.[918]

The investigative necessity requirement has been deemed to be one of the safeguards that allows Part VI of the *Criminal Code* to be constitutionally valid under s. 8 of the *Charter*.[919] However, Parliament's decision to remove the requirement in the context of the specific

[913] *Garofoli*, *supra* note 897 at 1444; *TELUS*, *supra* note 249 at para 27.
[914] See Section 5.3B) *supra* on this subject.
[915] *Criminal Code*, *supra* note 37, s 186(1)(b).
[916] *Araujo*, *supra* note 642 at paras 29, 33; *TELUS*, *supra* note 249 at para 28.
[917] NJ Whitling, "Wiretapping, Investigative Necessity, and the Charter" (2002) 46:1 Crim LQ 89 at 94.
[918] *Ibid* at 97; Cruess, *supra* note 860 at 63–64.
[919] *Araujo*, *supra* note 642 at para 26; *Duarte*, *supra* note 607 at 45; *Garofoli*, *supra* note 897 at 1444.

offences listed under s. 186(1.1) of the *Code*,[920] has been determined to be constitutionally valid, due to the presence of the condition that the authorization should only be issued when the judge is convinced that it is in the best interests of the administration of justice to do so.[921]

In *Duarte*, the SCC stated that the investigative necessity requirement reflects the fact that electronic surveillance should be used as a last resort investigative mechanism.[922] However, this is difficult to reconcile with *Araujo*, in which the SCC noted, quite to the contrary, that "a pure last resort test would turn the process of authorization into a formalistic exercise that would take no account of the difficulties of police investigations targeting sophisticated crime."[923] The interpretation of the investigative necessity requirement by the SCC in *Araujo* has been criticized as not providing sufficient protection to privacy, in light of the fact that courts seem to grant wiretap authorizations quite easily to law enforcement.[924] In any case, what is clear is that "[t]he rationale underlying this rule of investigative necessity is simple. If the same investigative ends can be accomplished by less intrusive means, then there is no rational justification for the added degree of intrusion occasioned by the use of electronic interception."[925]

---

[920] Namely: participation in activities of criminal organization (467.11); recruitment of members by a criminal organization (467.111); commission of offence for criminal organization (467.12); instructing commission of offence for criminal organization (467.13); offences committed for the benefit of, at the direction of or in association with a criminal organization; or terrorism offences.

[921] S. 186(1.1) of the Code has been deemed constitutional by multiple courts, including at the appellate level. See Hubbard, Brauti & Fenton, *supra* note 853, s 4:20. However, this conclusion has been criticized. See *inter alia* Whitling, *supra* note 917, who concludes that the investigative necessity requirement is constitutionally significant when it comes to the validity of Part VI of *the Criminal Code*.

[922] *Duarte*, *supra* note 607 at 55 referring to *R v Playford*, [1987] CCC (3d) 142 at 185.

[923] *Araujo*, *supra* note 642 at para 29.

[924] Cruess, *supra* note 860.

[925] Whitling, *supra* note 917 at 92. As the goal of the current part of this thesis is to analyze the impact of encryption of wiretaps, the question of whether the SCC's interpretation of the investigative necessity requirement is indeed coherent with the protections found within the Charter is better left for another occasion.

iv. Interceptions in Exceptional Circumstances

Only when there is a risk of imminent harm, in an urgent situation, can private communications be intercepted lawfully by a law enforcement officer, without a court authorization, under s. 184.4 of the *Criminal Code*. The SCC examined the legality of this provision in *Tse* and came to the conclusion that the provision respected s. 8 of the *Charter*, due to the fact that it is only available in exigent circumstances to prevent serious harm and because the provision contains strict conditions and limitations.[926] This power is aimed at very limited situations, such as "hostage takings, bomb threats and armed standoffs."[927] As with any other situation where a search or seizure is conducted without a valid court authorization, the Crown will bear the onus of proving that the conditions set forth in s. 184.4 of the *Criminal Code* have been met,[928] and thus that s. 8 of the *Charter* was not infringed.[929]

In *Tse*, the Court nonetheless concluded that s. 184.4 of the *Criminal Code* violated s. 8 of the *Charter*, but only because it failed to impose accountability procedures to law enforcement.[930] Since then, this has been addressed and the Minister of Public Safety and Emergency

---

[926] *Tse*, *supra* note 879 at para 58.

[927] *Ibid* at para 28, citing Standing Senate Committee on Legal and Constitutional Affairs*, Proceedings of the Standing Senate Committee on Legal and Constitutional Affairs, No. 44, 3rd Sess.* (Standing Senate Committee on Legal and Constitutional Affairs, 34th Parl., 1993) at 44:10.

[928] *Tse*, *supra* note 879 at para 58.

[929] This thesis will adopt the position that compelled decryption can respect ss. 7 and 8 of the *Charter* if stringent conditions are respected by law enforcement prior to the obtention of a judicial authorization. If this is found to be incorrect and the suggested framework is found to infringe *Charter*-protected rights, it is conceded that this investigative technique could probably only be saved under s. 1 of the *Charter* in situations analogous to the ones described by the SCC in *Tse*. In this decision, the fact that s. 184.4 of the *Criminal Code* is only applicable in exigent circumstances was found to be determinative when it came to the validity of the provision. Because the framework suggested below is not limited to exigent circumstances, the reasoning from *Tse* would need to be applied at a later stage of the examination of the constitutional validity of a compelled decryption framework (i.e., at the s. 1 stage).

[930] *Ibid* at para 85.

Preparedness must prepare and publish a report annually that states how many times the provision has been used within the last year.[931]

In other urgent situations where there is no risk of imminent harm but where law enforcement would not be able to obtain a s. 186 authorization in a reasonable delay, law enforcement can use s. 188 of the *Criminal Code* to obtain a wiretap authorization in an expedited fashion. In this case, law enforcement will be able to obtain the authorization without having to present written arguments[932] but will still need to respect the "investigative necessity" requirement found in s. 186(1)(b) of the *Code*.[933] This authorization will be limited to a 36-hour period. Contrary to s. 184.4, s. 188 does not have a preventative nature and thus can only be used as an investigative tool by law enforcement.[934]

[931] *Criminal Code*, *supra* note 37, s 195(2.1).
[932] Rather, a s. 188 application will be conducted orally in order to expedite the process. See *Tse*, *supra* note 879 at para 71.
[933] *Ibid* at para 65.
[934] *Ibid* at paras 77–78.

CHAPTER 6 COMPARATIVE PRACTISES ON THE SUBJECT OF COMPELLED DECRYPTION AND UNLOCKING OF DEVICES (THE AMERICAN, AUSTRALIAN, AND ENGLISH APPROACHES)

The uniqueness of the Canadian experience with self-incrimination and unreasonable searches and seizures is made clearer when compared with other similar legal systems, namely the American, Australian, and English criminal justice systems. These countries were chosen specifically because of their common heritage with Canada when it comes to criminal law, but also because of very different ways they have chosen to deal with encryption, both when it comes to data at rest and data in transit.

This chapter will start with a quick overview of how self-incrimination is treated in the United States, England, and Australia, before doing the same exercise for unreasonable searches and seizures. The specific way these three systems have decided to approach the subject of encryption will then be examined in more details. The goal of this chapter is to draw inspiration from the different approaches, while also distinguishing them from what should be done in Canada. Accordingly, the focus of this chapter is mainly on the solutions to the "going dark" problem that have been implemented in these countries, rather than on the underlying rules that justify them.

6.1 The American, Australian, and English Counterparts to the Canadian Principle against Self-Incrimination

6.1.1 Self-Incrimination in the United States

The Fifth Amendment of the United States Constitution states that "[n]o person … shall be compelled in any criminal case to be a witness against himself."[935] The main drafter of the Amendment, James Madison, did not specify its fundamental scope and application, leaving its interpretation to the courts.[936] Like its Canadian counterpart, it has been said to be rooted in the abhorrence for self-incrimination that emerged in England following specific procedural rules that compelled individuals to swear an oath and to self-incriminate.[937] As such, the Amendment would have been included in the American Constitution because the framers believed that "unhampered law enforcement sacrificed 'other social objects of a free society.'"[938]

This Amendment has been interpreted as having constitutionalized the common law privilege against self-incrimination.[939] As such, it gives witnesses and accused individuals an absolute right to refuse to answer any question that may incriminate them by "pleading the Fifth," as it is often phrased in popular culture, movies and television shows. While it was previously understood as applying only in front of the courts, the Supreme Court of the United States

---

[935] As cited *inter alia* in *S (RJ)*, *supra* note 343 at para 67.

[936] Harrison Metz, "Your Device is Disabled: How and Why Compulsion of Biometrics to Unlock Devices Should Be Protected Under the Fifth Amendment Privilege" (2019) 53:2 Val U L Rev 427 at 431.

[937] Brenner, *supra* note 220 at 87, referring to Leonard W Levy, *Origins of the Fifth Amendment: The Right Against Self-Incrimination* (Oxford: Oxford University Press, 1968). See also Metz, *supra* note 936 at 434. However, this is also criticized, see, e.g., Katharine B Hazlett, "The Nineteenth Century Origins of the Fifth Amendment Privilege Against Self-Incrimination" (1998) 42 Am J Legal Hist 235.

[938] Metz, *supra* note 936 at 434.

[939] *S (RJ)*, *supra* note 343 at para 67.

established early on that the Fifth Amendment applies to interactions with law enforcement, as these situations limit individual freedom and implicate self-incrimination considerations.[940] The Amendment thus provides not only a privilege applicable in front of the courts, but also a general right to silence.

Simply put, the Fifth Amendment "protects a person… against being incriminated by his own compelled testimonial communication."[941] The Fifth Amendment therefore aims to achieve, albeit very differently and with a different reach, the same goal as s. 5 of the *Canada Evidence Act* and s. 13 of the *Charter*, by protecting against *testimonial* self-incrimination.[942] For the Fifth Amendment to be triggered, some form of compulsion must be present and the compelled individual must be serving as a witness against themselves, which means that the individual is being compelled to reveal self-incriminating evidence by way of testimony.[943] As Orin S. Kerr puts it:

> The privilege against self-incrimination applies when three conditions are met. First, the person must face legal compulsion to cooperate with the government. Second, the compelled conduct must be testimonial, which means that it must force a person to "disclose[] the contents" of her "own mind" and therefore "communicate" a "factual assertion" or "convey some information to the Government." Third, the compelled testimony must be incriminating, which means that the prospect of complying "must establish reasonable ground to apprehend danger to the witness from his being

[940] *Miranda v Arizona*, 384 US 436 (1966) at 467, referred to in Brenner, *supra* note 220 at 88.
[941] *Fisher v United States*, 425 US 391 (1976) at 409 [*Fisher*], cited in Ajello, *supra* note 20 at 453.
[942] Some distinctions also exist between the two systems when it comes to the definition of the term *incrimination*. These distinctions will not be explained here, due to the limited use that will be made in this thesis of the American jurisprudence on self-incrimination.
[943] Chase Bales, "Unbreakable: The Fifth Amendment and Computer Passwords" (2012) 44 Ariz St LJ 1293 at 985 at 1294. Another way of seeing it is that the Fifth Amendment is triggered when a person is (1) compelled, (2) in a criminal case, (3) to be a witness, (4) against him or herself. See Robert H Cauthen, "The Fifth Amendment and Compelling Unencrypted Data, Encryption Codes, and Passwords" (2017) 41 Am J Trial Advoc 119 at 120.

> compelled to answer." A court must recognize an individual's privilege and block the government's effort to compel compliance only when all three conditions are satisfied.[944]

The protection granted by the Fifth Amendment can also be extended to the production of documents or other evidence, if the production of the evidence "conveys a statement of fact that certain documents are under the defendant's control or possession, or are authentic."[945] This is called the "act-of-production doctrine."[946] Otherwise, voluntarily prepared documents can be validly subpoenaed, even if their content is incriminating, under the "private papers doctrine."[947] The question that will need to be answered to determine if the act of production is testimonial in nature is "whether producing the evidence signifies a link in the evidentiary chain by providing the government with information they did not previously have."[948] This doctrine is very much aligned with the comments made by the SCC regarding the testimonial and communicative aspects of being compelled to produce pre-existing real evidence, which triggers the protection against self-incrimination even in a context where the documents were created voluntarily by the witness prior to the compulsion by the state.[949]

However, an important caveat attaches to the act-of-production doctrine in the United States. Under what is called the "foregone conclusion doctrine," defendants can be compelled to produce the documents, even if the production can be characterized as testimonial under the

---

[944] Kerr, *supra* note 3 at 5 (references omitted).
[945] Atwood, *supra* note 9 at 413. See also Bales, *supra* note 943 at 1295, referring to *Schmerber v California*, 384 US 757 (1966).
[946] Atwood, *supra* note 9 at 413.
[947] McGregor, *supra* note 6 at 587.
[948] Raila Cinda Brejt, "Abridging the Fifth Amendment: Compelled Decryption, Passwords, & Biometrics" (2021) 31:4 Fordham Intell Prop Media & Ent LJ 1154 at 1162.
[949] *BC Securities*, *supra* note 376 at para 47. See also Section 4.2.8 *supra*.

act-of-production doctrine, "if the government can demonstrate that it had prior knowledge of the existence, possession, or authenticity of the documents."[950] In other words, the compelled production of documents will be valid if the "existence and location [of the documents] are a foregone conclusion and [defendant's act of production] adds little or nothing to the sum total of the Government's information."[951] This knowledge by the state effectively annihilates the testimonial aspect of the production of the document, making the Fifth Amendment inapplicable, as it becomes "a matter of surrender rather than testimony."[952] However, the foregone conclusion will not be applicable if the authorities are simply presuming that the defendant has incriminating documents or are conducting a "fishing expedition."[953] The standard applicable to determine if the foregone conclusion doctrine is applicable is the "reasonable particularity" standard.[954] Similarly, the state cannot compel a defendant to create new documents or assemble evidence to respond to a *subpoena*, as this forces the defendant "to make extensive use of 'the contents of his own mind' in identifying the hundreds of documents responsive to the requests in the *subpoena*."[955] In other words,

> A defendant can be compelled to produce material evidence that is incriminating… But can he be compelled to use his mind to assist the prosecution in convicting him of a crime? I think not. He may in some cases be forced to surrender a key to a strongbox

[950] Atwood, *supra* note 9 at 413.
[951] *Ibid* citing *Fisher*, *supra* note 941 at 411.
[952] Brejt, *supra* note 948 at 1162.
[953] Atwood, *supra* note 9 at 416, referring to *United States v Hubbell*, 30 US 27 (2000).
[954] Brejt, *supra* note 948 at 1164, referring to *United States v Hubbell*, *supra* note 953, in which the Supreme Court of the United States referred to a Second Circuit case in which it was established that "the government must establish its knowledge of the existence, possession, and authenticity of subpoenaed documents with 'reasonable particularity' before the communication inherent in the act of production can be considered a foregone conclusion."
[955] Bales, *supra* note 943 at 1299 referring to *United States v Hubbell*, *supra* note 953 at 43.

> containing incriminating documents, but I do not believe he can be compelled to reveal the combination to his wall safe — by word or deed.[956]

Self-incrimination in the United States is often described as involving a "cruel trilemma":

> Whenever a suspect is asked for a response requiring him to communicate an express of implied assertion of fact or belief, the suspect confronts the 'trilemma' of truth, falsity, or silence [when silence carries a penalty], and hence the response (whether based on truth or falsity) contains a testimonial component.[957]

The Fifth Amendment aims to protect defendants against this cruel trilemma, by providing them with a right to refuse to answer the questions (or to provide the evidence of testimonial nature) that may incriminate them. However, the protection provided by the Fifth Amendment has been considerably weakened by the foregone conclusion doctrine, which does not have an equivalent in Canadian criminal law. Further, even when the Fifth Amendment is deemed applicable, the prosecution can override self-incrimination considerations by granting use and derivative use immunity to the defendant.[958]

In her *Stillman* dissent, Justice McLachlin gave a quick overview of the application of the Fifth Amendment, in the context of real evidence. According to this analysis, the Supreme Court of the United States has ruled that the privilege against self-incrimination does not extend to material evidence, as this type of compulsion is rather to be analyzed under the Fourth Amendment, which contains the guarantee against unreasonable search and seizure.[959]

---

[956] *Doe v United States*, 487 US 201 (1988) at 219 cited in Cohen & Park, *supra* note 3 at 181.
[957] *Pennsylvania v Muniz*, 496 US 582 (1990) at 597 cited in Bales, *supra* note 943 at 1297.
[958] Brenner, *supra* note 220 at 87. The Supreme Court of the United States decided in *Kastigar v United States*, 406 US 441 (1972) that the immunity must be "coextensive with the Fifth Amendment privilege," which has been interpreted as requiring use and derivative use immunity. See Hanni Fakhoury, "The Fifth Amendment and Privilege against Compelled Decryption" (2012) 9 Digital Evidence & Electronic Signature L Rev 81 at 83.
[959] *Stillman*, *supra* note 353 at paras 209–211.

Accordingly, the protection provided by the Fifth Amendment "does not apply to nontestimonial evidence such as fingerprints, blood, speaking certain words, handwriting samples, lineups, photo arrays, and show-ups (that is, evidence utilized primarily to identify people and connect them to the crime)."[960]

While the American experience with self-incrimination is interesting from a policy perspective, it must be kept in mind that the American approach has explicitly been considered but rejected in Canada.[961] Accordingly, the American experience with self-incrimination when it comes to the "going dark" debate is not necessarily relevant when it comes to the determination of whether the principle against self-incrimination in Canada protects against compelled decryption, but the solutions this country implemented to resolved this debate might be.

6.1.2 Self-Incrimination in England

The English position regarding the privilege against self-incrimination has been described by Iacobucci J. as "resting somewhere in between the Canadian and the American positions, inasmuch as the common-law privilege has not always been available in England, and inasmuch as it has not always been replaced by a co-extensive immunity."[962] As such, the principle against self-incrimination in the United Kingdom (UK) is limited, even when it comes to testimonial compulsion, as multiple statutes require individuals to answer questions and produce evidence.[963] Further, because the principle emanates purely from the common

[960] Cauthen, *supra* note 943 at 122.
[961] *S (RJ)*, *supra* note 343 at para 136, *in fine*; *Thomson Newspapers Ltd v Canada*, *supra* note 345 at 538.
[962] *S (RJ)*, *supra* note 343 at para 68.
[963] Chris Blair, "Miranda and the Right to Silence in England" (2003) 11:1 Tulsa J Comp & Int'l L 1 at 11.

law, and thus there is no written guarantee against self-incrimination in this country that does not have a written constitution, it is more easily subject to change.[964]

As with its Canadian and American offspring, the right against self-incrimination in the UK is said to take roots in the abolition of the Star Chamber and the distaste for compelling individuals to have to take an oath and testify against themselves.[965] As such, accused individuals are not compellable at their trials in England but are now competent to appear voluntarily.[966] The right against self-incrimination would then have evolved out of the courtroom to extend to the right to refuse to answer questions asked by law enforcement and the principle that involuntary confessions made to law enforcement should be excluded from evidence.[967] The right to silence in this context is justified, as in Canada and the United States, by the fact that individuals do not have a legal obligation to answer police questions, which is reflected in the cautions given to a detained individual before police questioning.[968] However, the right to consult with an attorney is much more limited in England, as it is not a part of the warnings given to suspects and the request to do so is often ignored by law enforcement, or simply not made by suspects.[969]

One other major difference between, on one side, the Canadian and American approaches, and on the other side, the English approach, is the consequences of the silence of the accused. As mentioned, in Canada no negative inferences can be drawn from the accused's silence at

[964] Mark Berger, "Rethinking Self-Incrimination in Great Britain" (1984) 61:3 Denver L Rev 507 at 508.
[965] *Ibid* at 508–509.
[966] *Ibid* at 540.
[967] *Ibid* at 510–511.
[968] *Ibid* at 519.
[969] *Ibid* at 539–540.

trial or during police interrogation.[970] The same prevails in the United States.[971] However, England has modified the common law rule on this subject in 1994 and has codified various negative inferences that can be drawn from the silence of the accused.[972] As described by Mark Berger:

> The structure adopted by the British legislation focused on both refusals by suspects to answer questions during police interrogations and criminal defendants who declined to testify at trial. In all such cases, warnings are given that adverse inferences may be drawn from the exercise of the right to silence. In the context of police interrogations, this may occur if an individual failed to account for an object, substance, or mark on his person, clothing, footwear, or in his possession; did not explain his presence at the scene where a crime had been committed at or about the time of his arrest; or failed to mention any fact later relied up at trial that he could reasonably have been expected to disclose at the time of his questioning by police. Adverse inferences could also be drawn against a criminal defendant who declined to take the witness stand at trial following a warning of the potential consequences of that decision. Where the [Criminal Justice and Public Order] Act applied, the fact finder was permitted to draw any "proper" inference from the individual's silence, although the adverse inference could not be the sole basis for a finding of guilt.[973]

This modification of the common law rule has been said by one author to be "a successful and balanced compromise between the need to protect the individual during the criminal process

---

[970] *Noble*, *supra* note 482 at para 75.
[971] Constantine Theophilopoulos, "The Influence of American and English Law on the Interpretation of the South African Right to Silence and the Privilege against Self-Incrimination" (2005) 19:2 Temple Int'l & Comp LJ 387 at 388 referring to *Miranda v Arizona*, *supra* note 940. See also Blair, *supra* note 963 at 3–9.
[972] Albert W Alschuler, "A Peculiar Privilege in Historical Perspective: The Right to Remain Silent" (1995) 94 Mich L Rev 2625 at 2667; Mark Berger, "Europeanizing Self-Incrimination: The Right to Remain Silent in the European Court of Human Rights" (2006) 12:2 Colum J Eur L 339 at 373.
[973] Berger, *supra* note 972 at 373–374.

and the need to combat crime in the most efficient manner possible,"[974] while others have criticized this choice.[975]

Following these changes, individuals in the UK retain a right to remain silent, as there is no new offense committed when an individual refuses to answer law enforcement's questions, but a severe burden is placed on the exercise of that right.[976] They also maintain the traditional common law privilege against self-incrimination and the ability to refuse to answer self-incriminating questions at trial (with exceptions), but a negative inference can similarly be drawn from that decision.[977] To some degree, the adverse inferences that can be drawn in the UK when the prosecution's evidence requires a response from the accused at trial are aligned with Lamer J.'s comments *R v P (MB)* about the tactical necessity for the accused to present evidence or to testify once the prosecution has established their case to meet.[978]

The European Court has recognized the right to remain silent as being included under article 6(1) of the *European Convention on Human Rights* (*ECHR*), which was ratified in the UK in 1951 and later incorporated in English law by the *Human Rights Act* of 1998,[979] despite not

---

[974] Theophilopoulos, *supra* note 971 at 394.

[975] John D Jackson, "Silence and Proof: Extending the Boundaries of Criminal Proceedings in the United Kingdom" (2001) 5:3 Int'l J Evidence & Proof 145; Mark Berger, "Reforming Confession Law British Style: A Decade of Experience with Adverse Inferences from Silence" (2000) 31:2 Colum Hum Rts L Rev 243.

[976] Blair, *supra* note 963 at 14.

[977] Ian H Dennis, "Rectitude Rights and Legitimacy: Reassessing and Reforming the Privilege against Self-Incrimination in English Law" (1997) 31:1–3 Isr L Rev 24 at 54.

[978] *P (MB)*, *supra* note 367 at 579.

[979] Blair, *supra* note 963 at 17. This has not been impacted by Brexit. See "The Supreme Court and Europe - What is the relationship between the UK Supreme Court, the European Court of Human Rights, and the Court of Justice of the European Union?", (2022), online: *Supreme Court* <https://www.supremecourt.uk/about/the-supreme-court-and-europe.html>. However, the UK has mentioned a possible withdrawal from the ECHR in 2022. This has not been done as of now. See Andrew Sparrow, "No 10 revives prospect of UK leaving European convention on human rights after Labour calls Rwanda plans 'a shambles' - as it happened", (15 June 2022), online: *The Guardian* <https://www.theguardian.com/politics/live/2022/jun/15/rwanda-flight-asylum-echr-priti-patel-boris-johnson-pmqs-uk-politics-latest>.

being explicitly mentioned in the text, as part of fair-hearing rights.[980] The Court also established that the right to remain silent is also linked to the presumption of innocence and the burden of proof in criminal cases:

> The right not to incriminate oneself, in particular, presupposes that the prosecution in a criminal case seek to prove their case against the accused without resort to evidence obtained through methods of coercion or oppression in defiance with the will of the accused. In this sense the right is closely linked to the presumption of innocence contained in Article 6 para. 2 of the Convention.[981]

However, the Court has not defined precisely the reach of the Convention's self-incrimination right.[982] Nonetheless, what is clear is that self-incrimination considerations are relevant in Europe when it comes to determining the validity of procedural rules, but in a much more limited manner than in the United States or in Canada, even though the Court's analysis of Article 6 of the Convention can be seen as expanding the right against self-incrimination. [983] On the other side, the UK has been doing the opposite through its legislation on adverse inferences, which is surprising considering that the search for truth is historically more important in continental Europe than in common law systems.[984] However, the various inferences that can be drawn from the accused's silence in the UK have also been determined

---

[980] Berger, *supra* note 972 at 342–343.

[981] *Saunders v United Kingdom*, App No 14310/88, 23 Eur HR Rep 313 (1996), cited in Berger, *supra* note 972 at 344.

[982] Berger, *supra* note 972 at 345.

[983] Dennis, *supra* note 977 at 25–27. According to the author, two main reasons explain the decline of the protection against self-incrimination in England. First, some people view it as impeding law enforcement's legitimate interest in uncovering the truth of a case. This perspective resembles Bentham's vision on the privilege against self-incrimination and can also be analyzed through Packer's 'Crime Control Model.' This would also be the main reason behind the adoption of the legislation concerning adverse inferences in England. Second, the privilege against self-incrimination is only one of the methods of protecting accused individuals, making its modification possible.

[984] Robert S Gerstein, "The Self-Incrimination Debate in Great Britain" (1979) 27:1 Am J Comp L 81 at 82.

to be in accordance with the *European Convention on Human Rights*, as long as a conviction is not based solely or mainly on the inferences drawn from the silence of the accused.[985] Proper instructions to the jury are also necessary and the circumstances at play must warrant the inferences being drawn, including if the individual was provided with legal counsel and what advice was actually provided by counsel.[986]

The UK courts have rejected the idea that the principle against self-incrimination could be used to protect individuals against the obligation to provide bodily evidence, preferring to consider this type of practise under the principle against unreasonable search and seizure.[987] This is similar, to some degree, to the preference that the SCC has shown to consider non-testimonial self-incrimination under s. 8 of the *Charter*.

6.1.3 Self-Incrimination in Australia

The Australian Constitution does not contain provisions regarding fundamental rights and freedoms. Australia does however recognize the principle against self-incrimination as being fundamental, through its common law heritage. Australian courts have interpreted this principle as conferring a limited right against compelled testimony, not against any type of compulsion.[988] Accordingly, non-testimonial evidence, such as fingerprints or DNA samples, is not protected by the principle against self-incrimination in Australia, while the compelled production of documents is.[989]

---

[985] Berger, *supra* note 972 at 374.
[986] *Ibid* at 375–377.
[987] *Stillman*, *supra* note 353 at para 212 (Justice McLachlin's dissenting reasons).
[988] *Ibid* at paras 213–215 (Justice McLachlin's dissenting reasons).
[989] Australian Law Reform Commission, *Traditional Rights and Freedoms - Encroachments by Commonwealth LS; Final Report* (Sydney: Australian Law Reform Commission (ALRC), 2015) at 312.

The idea that the principle against self-incrimination can be used to achieve balance between opposed interests in the criminal justice system has also been recognized in Australia. As described by the Australian Law Reform Commission (ALRC):

> A number of rationales have been said to underpin the privilege. In recent judgments, it has been said to be necessary to preserve the proper balance between the powers of the state and the rights and interests of citizens, to preserve the presumption of innocence and to ensure that the burden of proof remains on the prosecution. At other times, the courts have described the privilege as a human right, necessary to protect the privacy, freedom and dignity of the individual.[990]

Australia's High Court has recognized that the privilege against self-incrimination is only a part of the broader principle that the burden of proof to establish the guilt of the accused rests on the prosecution:

> Our system of criminal justice reflects a balance struck between the power of the State to prosecute and the position of an individual who stands accused. The principle of the common law is that the prosecution is to prove the guilt of an accused person. This was accepted as fundamental in *X7*. The principle is so fundamental that "no attempt to whittle it down can be entertained" albeit its application may be affected by a statute expressed clearly or in words of necessary intendment. The privilege against self-incrimination may be lost, but the principle remains. The principle is an aspect of the accusatorial nature of a criminal trial in our system of criminal justice.
>
> The companion rule to the fundamental principle is that an accused person cannot be required to testify. The prosecution cannot compel a person charged with a crime to assist in the discharge of its onus of proof.[991]

---

[990] *Ibid* at 310. While the ALRC here refer to the "privilege" against self-incrimination, it seems applicable to a more general "principle" against self-incrimination.

[991] *Lee v The Queen*, [2014] HCA 20 at paras 32–33 cited in Australian Law Reform Commission, *supra* note 989 at 315.

The traditional common law privilege against self-incrimination is still generally applicable in Australia. The Australian *Uniform Evidence Acts* contain provisions conferring the right to resist disclosure of information in judicial proceedings. However, other statutes have removed the privilege by establishing powers to compel individuals to answer questions, based on the public interest in investigating crimes. Usually, these statutes will provide use immunity (or sometimes even derivative use immunity) to the person compelled to give self-incriminating evidence. Further, Australian courts also have the possibility of excluding evidence that would render the trial unfair, including for self-incrimination reasons.[992]

Australian courts consider the privilege against self-incrimination in a similar way to Canadian courts. As such, the privilege is seen as reflecting "the long-standing antipathy of the common law to compulsory interrogations about criminal conduct."[993] Like the English, Canadian, and American versions of the privilege, the Australian principle is applicable to resist the compelled production of documents and the compulsion to make declarations to law enforcement before trial (i.e., right to silence), or to the court at trial (i.e., privilege against self-incrimination).[994] For this reason, the way this country has decided to regulate compelled decryption is especially interesting, although the Canadian experience with self-incrimination provides broader protection against compulsion of incriminating evidence.

[992] Australian Law Reform Commission, *supra* note 989 at 310.
[993] *Lee v New South Wales Crime Commission* (2013) 302 ALR 363 cited in Australian Law Reform Commission, *supra* note 989 at 311.
[994] Australian Law Reform Commission, *supra* note 989 at 311.

6.2 THE AMERICAN, AUSTRALIAN, AND ENGLISH COUNTERPARTS TO THE CANADIAN PROTECTION AGAINST UNREASONABLE SEARCH AND SEIZURE

Common law countries share the common root of having search and seizure protections that were originally strongly influenced by the notion of private property and the law of trespass.[995] They also share some basic search and seizure requirements, namely probable cause, particularity, and reliability of evidence, with some exceptions to their application.[996] However, these systems have nonetheless evolved independently to reach different visions of what constitutes an unreasonable search or seizure. This section will provide a brief overview of how the United States, the UK, and Australia now treat unreasonable searches of seizures.

6.2.1 Unreasonable Search and Seizure in the United States

The SCC in *Hunter* analyzed in a fairly extensive manner the American vision of the right to be secure against unreasonable search and seizure. Effectively, the Canadian approach originally crafted in *Hunter* is largely based on the American jurisprudence regarding the Fourth Amendment of the United States Constitution, which is the counterpart to s. 8 of the *Charter*. As such, both systems are based on the existence of a reasonable expectation of privacy and the idea that the protection against unreasonable search and seizure has outgrown its origins within property law, to now "[protect] people, not places."[997] Further, both the Fourth Amendment and s. 8 of the *Charter* aim to impose procedural constraints on

[995] *Hunter*, *supra* note 31 at 157.
[996] R Thomas Farrar, "Aspects of Police Search and Seizure Without Warrant in England and the United States" (1974) 29 U Miami L Rev 491 at 496.
[997] *Katz v United States*, *supra* note 559, cited in *Hunter*, *supra* note 31 at 159.

governmental access to information.[998] As it is the case in Canada, warrantless searches or seizures are also presumed unreasonable in the United States.[999]

One major difference between the American and Canadian visions of the protection against unreasonable search and seizure is found within the American "third-party doctrine" which states that information shared with a third party can no longer attract a reasonable expectation of privacy.[1000] As stated previously, this does not apply in Canada, as control is only one of the factors to consider in the establishment of a reasonable expectation of privacy.[1001] As such, law enforcement in the United States does not need to acquire a warrant to obtain data that is shared with a third-party. Further, the Fourth Amendment has been interpreted as not applying to physical characteristics, such as fingerprints, in the context where the characteristic is being sought-after for identification purposes, rather than investigative purposes.[1002]

Interestingly, the Supreme Court of the United States adopted a completely different approach than the SCC to the search of devices incident to arrest in *Riley v California*.[1003] Following this decision, law enforcement needs a warrant in order to access the contents of a device, even when the device is seized incident to a lawful arrest.[1004]

---

[998] Choi, *supra* note 537 at 193.
[999] John ED Larkin, "Compelled Production of Encrypted Data" (2012) 14 Vanderbilt J Ent & Tech L 253 at 259.
[1000] Choi, *supra* note 537 at 188; Opderbeck, *supra* note 3 at 1668. See also *Plant*, *supra* note 565 at 293.
[1001] See for example *Marakah*, *supra* note 260 at para 130.
[1002] Opher Shweiki & Youli Lee, "Compelled Use of Biometric Keys to Unlock a Digital Device: Deciphering Recent Legal Developments" (2019) 67 US Atty's Bull 23 at 26–27.
[1003] *Riley v California*, 573 US 373 (2014).
[1004] See *Fearon*, *supra* note 1 at para 60.

6.2.2 Unreasonable Search and Seizure in England

Generally, English law is fairly similar to Canadian law on this subject; warrants will be necessary in most cases to enter homes and other specific locations to find evidence, and police also have the power to conduct certain searches or seizures without a warrant, for example in the case of search incident to arrest. The development of the warrant requirement in England was linked to a desire to provide judicial control over police action, in a context where judges could not always be present at the scene of a search or a seizure.[1005]

Article 8 of the *ECHR* contains a protection against unjustified state interference in individuals' private and family lives. This provision dictates that:

> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. [1006]

As such, it can be seen as a mechanism to balance individual interests with valid state objectives, in a similar fashion than what is done under s. 8 of the *Charter*.[1007]

Under the *Police and Criminal Evidence Act 1984*, a warrant can be issued for the search of a specific location under the standard of *reasonable grounds to believe*.[1008] However, the

[1005] Farrar, *supra* note 996 at 501–502.
[1006] Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos 11 and 14*, 4 November 1950, ETS 5, s 8.
[1007] As mentioned *supra* at note 979, the applicability of the ECHR has not been impacted by Brexit but this may change as the UK has threaten to withdraw from the ECHR. See Sparrow, *supra* note 979.
[1008] *Police and Criminal Evidence Act 1984* (s. 66), UK Public General Acts, s 8.

lower standard of *reasonable grounds to suspect* will be applicable in different scenarios, such as when law enforcement wants to stop and search an individual suspected of carrying illegal drugs, weapons, stolen property, or objects that can be used to commit a crime.[1009] This lower standard was actually created in the UK and was the applicable standard to arrest an individual suspected of having committed a felony.[1010] Search powers enacted in 2016 now give law enforcement the right to access computers remotely in a covert manner, without a warrant.[1011] Some provisions were also enacted relating to compelled decryption of data.[1012] It also seems that, generally speaking, warrantless searches of cellular phones incident to arrest are permitted in the UK.[1013]

At common law, illegally obtained evidence was deemed admissible, if relevant and reliable.[1014] However, since the adoption of the *Police and Criminal Evidence Act 1984*, courts now have the discretionary power to refuse to allow evidence if it would negatively impact the fairness of the trial.[1015]

[1009] United Kingdom Government, "Police powers to stop and search: your rights", online: *GovUK* <https://www.gov.uk/police-powers-to-stop-and-search-your-rights>.
[1010] Terry Skolnik, "The Suspicious Distinction between Reasonable Suspicion and Reasonable Grounds to Believe" (2016) 47:1 Ott L Rev 227 at 231.
[1011] *Investigatory Powers Act 2016* (c. 25), UK Parliament, 2016.
[1012] *Regulation of Investigatory Powers Act 2000* (c. 23), UK Parliament, 2000.
[1013] Matthew Raj & Russ Marshall, "Examining the Legitimacy of Police Powers to Search Portable Devices in Queensland" (2019) 38:1 U Queensland LJ 99 at 102–103.
[1014] Debra Osborn, "Suppressing the Truth: Judicial Exclusion of Illegally Obtained Evidence in the United States, Canada, England and Australia" (2000) 7:4 Murdoch U Electron JL at para 31.
[1015] *Ibid* at paras 32–34.

6.2.3 Unreasonable Search and Seizure in Australia

Australia does not have a direct equivalent to the American Fourth Amendment or to s. 8 of the *Charter*.[1016] As such, privacy does not receive a constitutional protection[1017] and the expression "unreasonable search and seizure" does not seem to be used in Australia. Privacy seems rather to receive a protection of limited scope, by way of legislation applicable in specific sectors—when it comes to the collection of data on individuals by corporations for example.[1018] Similarly, the Australian common law does not contain a general right to privacy either.[1019] However, specific legislation will respect the general idea that strong privacy interests will require stringent conditions to be applied in order for those interests to be overcome by law enforcement's interest in investigating and prosecuting crime.[1020]

Criminal law in Australia operates at federal and state levels.[1021] The Australian *Crimes Act*, applicable at the federal level, contains provisions similar to s. 487(2.1) and (2.2) of the Canadian *Criminal Code* when it comes to the use of electronic devices at the location of a search or seizure. As such, officers executing a search warrant are expressly authorized to use the electronic equipment found within the searched premises and to copy the data located on the devices or that the devices give access to.[1022] Under this act, search warrants for specific

[1016] Paul Marcus & Vicky Waye, "Australia and the United States: Two Common Criminal Justice Systems Uncommonly at Odds" (2003) 12:1 Tulane J Int'l Comp L 27 at 38.
[1017] Roger Clarke, "Privacy Impact Assessment in Australian Contexts" (2008) 15 eLaw J 72 at 76.
[1018] See for example Australian Parliament, *Privacy Act 1988*, No 119, 1988, which is similar to Canada's *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 [*PIPEDA*]
[1019] Margaret Jackson, "Data Protection Regulation in Australia after 1988" (1997) 5:2 Int'l JL & Inf Tech 158 at 160.
[1020] Raj & Marshall, *supra* note 1013 at 104.
[1021] Marcus & Waye, *supra* note 1016 at 29.
[1022] Australia Parliament, *Crimes Act 1914*, No 12, 1914, s 3L. See also Dane Bryce Weber, "The Cybernetic Sea: Australia's Approach to the Wave of Cybercrime" (2014) 14 QUT L Rev 52 at 62–64.

locations can be obtained when law enforcement respect the *reasonable grounds to suspect* standard.[1023] This will also be the case in some state level criminal legislation,[1024] while others will rather use the *reasonable grounds to believe* standard.[1025] Depending on the state, different laws will apply to the seizure of cellular phones, whether for investigative purposes prior to arrest or incident to arrest. In Queensland for example, it seems that law enforcement agents can search devices before arrest, under certain conditions, but can only seize the device without searching it if it is done incidental to arrest.[1026] Australia also enacted compelled decryption legislation, which will be examined in more detail in Part 2.[1027]

Australian search and seizure laws—either at the federal or state level—are usually seen as granting powers to law enforcement, rather than protecting individuals against state interference.[1028] However, some protection derives from the fact that these provisions are usually interpreted in a fairly strict manner, making any search or seizure that fall outside of the scope of the provision unlawful.[1029] When a search or seizure is deemed unlawful, courts will have the discretionary power to exclude the evidence obtained illegally,[1030] in a somewhat similar manner than what is done in Canada under s. 24(2) of the *Charter*.

[1023] *Crimes Act 1914*, *supra* note 1022, s 3E.
[1024] For example, see Queensland Government, *Police Powers and Responsibilities Act 2000*, s 151.
[1025] For example, see Victoria Legislation, *Crimes Act 1958*, s 465; New South Wales Government, *Law Enforcement (Powers and Responsibilities) Act 2002*, No 103, s 47.
[1026] Raj & Marshall, *supra* note 1013 at 116.
[1027] Australia, *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, No. 148 (2018).
[1028] Marcus & Waye, *supra* note 1016 at 38.
[1029] *Ibid* at 39.
[1030] *Ibid* at 41.

6.3 The American, Australian, and English Approaches to Compelled Decryption and Unlocking of Devices

The United States, UK, and Australia have all heavily discussed the impact of encryption on criminal investigations in recent years. Even since the San Bernardino events in 2015 in California, encryption has been the subject of many articles and laws in the United States.[1031] The UK government has recently launched a campaign to militate against strong encryption used by Facebook (now Meta) on their various communications platforms, including E2EE currently used on WhatsApp but that could be rolled out to their other platforms, including Facebook Messenger.[1032] Australia is still in the thick of it, after adopting a highly controversial encryption law in 2018.[1033] While these countries share a common heritage when it comes to criminal law, they have adopted very different approaches to regulate what law enforcement can do to circumvent encryption.

6.3.1 The American Approach

No federal or state level legislation in the United States currently gives law enforcement the specific power to compel individuals to unlock their devices or decrypt their data. In the absence of any such legislation, compelled decryption imposed on suspects has rather been

[1031] Nakashima & Albergotti, *supra* note 100.

[1032] Joe Mullin, "The U.K. Paid $724,000 For A Creepy Campaign to Convince People That Encryption is Bad. It Won't Work.", (21 January 2022), online: *Electron Front Found* <https://www.eff.org/deeplinks/2022/01/uk-paid-724000-creepy-campaign-convince-people-encryption-bad-it-wont-work>.

[1033] See *inter alia* Paul Karp, "Australia's world-first anti-encryption law should be overhauled, independent monitor says", (9 July 2020), online: *The Guardian* <https://www.theguardian.com/australia-news/2020/jul/09/australias-world-first-anti-encryption-law-should-be-overhauled-independent-monitor-says>; Sam Bocetta, "Australia's New Anti-Encryption Law is Unprecedented and Undermines Global Privacy", (14 February 2019), online: *Found Econ Educ* <https://fee.org/articles/australia-s-unprecedented-encryption-law-is-a-threat-to-global-privacy/>; *The Encryption Debate in Australia: 2021 Update*, by Stilgherrian (Washington, DC: Carnegie Endowment for International Peace, 2021).

examined by the courts, mostly in relationship with the Fifth Amendment. Indeed, the Fourth Amendment seems to be of very limited help when it comes to the determination of whether law enforcement should be given the power to compel individuals to decrypt their data or unlock their devices, as most authors only examine the applicability of the Fifth Amendment to this situation. However, it has been suggested that the only way of properly addressing this situation is by reunifying both the Fourth and the Fifth Amendment, under the general proposition that these constitutional provisions were adopted to limit state power, not augment it.[1034]

As mentioned, the protection against self-incrimination in the United States has been interpreted as being limited to testimonial communications, including the act of producing evidence. As such, it does not afford any protection to material evidence, which has been found to be better considered under the Fourth Amendment. Accordingly, courts have adopted different reasonings depending on the encryption method used in the specific instance being examined.

A) Decryption by Suspect of Data at Rest – Alphanumeric Passwords

When it comes to alphanumeric passwords, the current state of the law in the United States originates from lower courts, in the absence of a decision from the Supreme Court of the United States that could provide some overarching guidance. These decisions distinguish generally between the method the state is seeking to use to reach the decrypted data: (1) compelling the defendant to verbally reveal their passwords; (2) compelling the defendant to provide a previously written document where the password had been noted; (3) compelling

[1034] Choi, *supra* note 537; Sacharoff, *supra* note 20. See Section 7.1 *infra*.

the production of a decrypted version of the data; or (4) compelling the defendant to physically enter the password directly into the device.

When it comes to compelling a defendant to verbally reveal their password, in *United States v Kirschner*, a Michigan district court decided that a suspect could not be compelled to reveal his passwords verbally, by testifying in front of a grand jury.[1035] In this case, the Court stated that "compelling [the defendant] to testify to the password is more like compelling him to provide the combination to the wall safe than the key to the strongbox containing incriminating documents,"[1036] which cannot be done under the Fifth Amendment. Further, the Court concluded that the immunities provided under the applicable status were insufficient to overcome the defendant's rights, as the password might lead to incriminating evidence.[1037] This analysis has been confirmed by other courts,[1038] albeit not unanimously.[1039]

When it comes to the other options of compelling the production of the decrypted data or of a document where the encryption key or password would have been previously noted, courts generally rely on the "act of production doctrine" and the "foregone conclusion doctrine." In *United States v Pearson*, a New York district court examined the possibility of compelling the defendant to produce a previously written document where the encryption key would have been noted. The Court concluded that the defendant had admitted that the password itself carried no testimonial value, as the defendant had instead claimed protection under the Fifth

[1035] *United States v Kirschner*, 823 F Supp 2d 665 (2010) cited in Bales, *supra* note 943 at 1302.
[1036] Cauthen, *supra* note 943 at 130, paraphrasing *United States v Kirschner*, *supra* note 1035 at 668–669.
[1037] Cauthen, *supra* note 943 at 130.
[1038] *In re Grand Jury Subpoena to Boucher*, 2009 WL 424718; *Commonwealth v Baust*, 89 Va Cir 267 (2014); *SEC v Huang*, 2015 WL 5611644, cited in Cohen & Park, *supra* note 3 at 185.
[1039] *State v Stahl*, 206 So 3d 124 (2016).

Amendment *via* the "act of production doctrine."[1040] The Court, however, did not decide if the act of decryption could be qualified as testimonial in this specific case, as the defendant pleaded guilty before the court could determine if the prosecution could authenticate the files found on the computer by other means than compelling the defendant to produce his password.[1041]

Nonetheless, *Pearson* provides an interesting perspective as to whether compelled decryption can be qualified as testimonial, under the "act of production doctrine." It effectively opened the door to the possibility that passwords can receive no protection under the Fifth Amendment, if the government can satisfy the "foregone conclusion doctrine," or if it can prove that the defendant has written down the password to his device in another location, making the production of that piece of paper or note compellable. Further, in this case, the Court opined that the presence of documents on the computer that did not belong to the defendant was a relevant factor to consider when determining whether the act of decryption can be qualified as testimonial, as it would create a risk that the defendant would falsely authenticate data found on the computer as his own by providing the password for the device.[1042]

In *In re Grand Jury Subpoena to Boucher*, a case where the accused's computer was seized at the Canada-United States border, the prosecution tried to compel the production of a decrypted version of the files legally seized by the border agents, instead of compelling the accused to provide his password.[1043] The subpoena was eventually confirmed, as the Court

[1040] *United States v Pearson*, 2006 US Dist LEXIS 32982, cited in Cauthen, *supra* note 943 at 131.
[1041] McGregor, *supra* note 6 at 594.
[1042] Bales, *supra* note 943 at 1301.
[1043] *In re Grand Jury Subpoena to Boucher*, *supra* note 1038, cited in Cauthen, *supra* note 943 at 132.

determined that the contents of the laptop had been voluntarily prepared and that the "foregone conclusion doctrine" was applicable in this instance, due to the fact that the border agents had previously seen the contents of the device before the encryption mechanism had been activated.[1044] According to the court, the application of the "foregone conclusion doctrine" rests on the fact that the state can demonstrate that it knows about the location and existence of the documents, not their contents.[1045] Consequently, the act of producing the decrypted material was deemed to add nothing to the government's case against the accused.

Similarly, in *United States v Fricosu*, the government sought to compel the production of decrypted versions of the data found on validly seized computers.[1046] In this case, the defendant had recognized ownership of the devices and that she knew that the files were password protected. The Court, relying on *Boucher*, concluded that the contents of the computer had been voluntarily prepared and that the "foregone conclusion doctrine" allowed the government to overcome the testimonial aspect of decryption, brought forward by the "act of production doctrine."[1047] Interestingly, the Court granted immunity towards the defendant, in regard to the act of producing the decrypted documents.[1048]

In an Eleventh Circuit decision, *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, the Court concluded that both production and decryption of hard drives were of

[1044] *In re Grand Jury Subpoena to Boucher*, *supra* note 1038, cited in Cauthen, *supra* note 943 at 133–134.
[1045] McGregor, *supra* note 6 at 595.
[1046] *United States v Fricosu*, 841 F Supp 2d 1232 (D Colo 2012), *appeal denied by, stay denied by* Fricosu v United States, No. 12-701, 2012 US App LEXIS 3561 (10th Cir Feb 2012), cited in Cauthen, *supra* note 943 at 134.
[1047] Cauthen, *supra* note 943 at 134–135.
[1048] *Ibid* at 135. The suggestions made later on in Chapter 7 will rely on a similar act of production immunity, which is inspired from *Fricosu*, *supra* note 1046.

testimonial nature.[1049] As such, in order to validly compel production of the decrypted data, the prosecution would need to rely on the "foregone conclusion doctrine." The Court concluded that in order for the doctrine to apply, the Government needed to show prior knowledge of the existence and location of the files on the devices.[1050] In this specific instance, the Court determined that the "foregone conclusion doctrine" requirements had not been satisfied by the prosecution, as it had "failed to show with reasonable particularity that it knew any files existed at all, knew any files were located on the encrypted hard drives, could independently authenticate any such files, or that [the accused] could access and decrypt any such files."[1051] One major obstacle to the application of the "foregone conclusion doctrine" was that the prosecution could not prove that the device had anything on it, as the encryption software used (TrueCrypt) created hidden volumes.[1052] The Court also stated that the applicable legislative immunities were insufficient, as it did not provide with "act of production" immunity.[1053] A similar result was reached in other decisions.[1054]

In *Commonwealth v Gelfgatt*, the prosecution sought to compel the defendant to enter his password directly into four computers he admitted being able to decrypt.[1055] The defendant was using DriveCrypt plus, an encryption software that can only be circumvented by entering

[1049] *In Re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F3d 1335 (2012), cited in Bales, *supra* note 943 at 1302. See also Cohen & Park, *supra* note 3 at 187–190.
[1050] Bales, *supra* note 943 at 1302.
[1051] Cauthen, *supra* note 943 at 136.
[1052] Jarone, *supra* note 46 at 787.
[1053] *In Re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, *supra* note 1049, cited in Cauthen, *supra* note 943 at 136–137.
[1054] *United States v Apple MacPro Computer*, 851 F3d 238 (2017), cited in Cauthen, *supra* note 943 at 138–139; *In re The Decryption of a Seized Data Storage System (Feldman)*, 2013 US Dist LEXIS 202353, cited in Cohen & Park, *supra* note 3 at 190.
[1055] *Commonwealth v Gelfgatt*, 11 NE3d 605 (2014), cited in Cohen & Park, *supra* note 3 at 191–192.

the pre-designated passcode.[1056] The Court recognized that the act of entering passwords into a device was of testimonial nature (because it admitted ownership and control over the computers) but concluded that the prosecution had satisfied the requirement of the "foregone conclusion doctrine," making the Fifth Amendment inapplicable.[1057] Interestingly, in his dissenting reasons, Judge Lenk mentioned that the fact that the accused was an attorney should have been considered, as forcing him to decrypt the devices would result in a breach of his attorney-client privilege. Judge Lenk would have concluded that the prosecution did not satisfy the "foregone conclusion doctrine," because it could not show sufficient knowledge of the location of the data due to the fact that the accused had used cloud computing services to store his data.[1058]

B) Decryption by Suspect of Data at Rest – Biometric Protection Methods

Generally speaking, courts in the United States have concluded that the Fifth Amendment affords no protection whatsoever to data protected with biometric protection methods, whether facial or digital recognition, on the motive that the Fifth Amendment does not apply to bodily evidence.[1059]

However, other courts have adopted a more forward-looking approach and concluded that compelling a suspect to unlock a cellphone with a biometric feature can indeed be qualified

[1056] Minerva Pinto, "The Future of the Foregone Conclusion Doctrine and Compelled Decryption in the Age of Cloud Computing" (2016) 25:1 Temp Pol & Civ Rts L Rev 223 at 225.
[1057] Cohen & Park, *supra* note 3 at 192.
[1058] Pinto, *supra* note 1056 at 223, referring to *Commonwealth v Gelfgatt*, *supra* note 1055 at 534–536.
[1059] *Matter of Search Warrant Application for [redacted text]*, 2017 WL 4563861; *State v Diamond*, 890 NW2d 143 (2017); *Commonwealth v Baust*, *supra* note 1038; *State v Stahl*, *supra* note 1039, cited in Blanch & Christensen, *supra* note 3 at 6; *Barrera*, 2019 WL 6253812; *In Re Search of a White Google Pixel 3XL Cellphone in a Black Incipro Case*, 398 F Supp 3d 785 (D Idaho 2019), cited in Redfern, *supra* note 215 at 615.

as testimonial under the Fifth Amendment, because it communicates information, such as prior access to the device.[1060] Following the Supreme Court of the United States reasoning in *Riley v California*[1061] and subsequent decision *Carpenter v United States*,[1062] these decisions recognize that cellphones are exceptional and different from any other object that might be of interest for law enforcement.[1063] In *Riley*, the Supreme Court went as far as stating that "the proverbial visitor from Mars might conclude [cellphones] were an important feature of human anatomy,"[1064] requiring us to view cellphones in a unique way that recognizes the unique privacy considerations they raise.

C) Decryption by TPDC of Data in Transit

Throughout the years, several bills have been introduced in the United States in order to limit encryption capacities directly at the source, by imposing decryption capabilities on TPDCs directly. For example, the *Lawful access to Encrypted Data Act* (*LAED Act*)—introduced in 2020 but never adopted—aimed to ensure that TPDCs could access the plaintext of encrypted data, whether it was data in motion or data at rest.[1065] As it currently stands however, only telecommunications service providers need to maintain the ability the decrypt

[1060] *In Re Application for a Search Warrant*, 236 F Supp 3d 1066 (2017), cited in Blanch & Christensen, *supra* note 3 at 7; Cohen & Park, *supra* note 3 at 195–196; *Seo v State*, 109 NE 3d 418 (2018); *In re Search of Residence in Oakland, CA*, 354 F Supp 3d 1010 (2019), cited in Bryan H Choi, "The Privilege against Cellphone Incrimination" (2018) 97 Tex L Rev Online 73 at 74; *Matter of Single-family Home & Attached Garage*, 2017 WL 4563870; *United States v Wright*, 2020 WL 60239, cited in Redfern, *supra* note 215 at 617.
[1061] *Riley v California*, *supra* note 1003.
[1062] *Carpenter v United States*, 138 S Ct 2206 (2018).
[1063] Choi, *supra* note 1060 at 75.
[1064] *Riley v California*, *supra* note 1003 at 2484, cited in Choi, *supra* note 1060 at 75.
[1065] United States 116th Congress, *Lawful Access to Encrypted Data Act*, s 4051 (2019-2020).

communications, under the *Communications Assistance for Law Enforcement Act* (*CALEA*).[1066]

CALEA was adopted in 1994 with the specific goal of making sure law enforcement would maintain the ability to wiretap communications.[1067] CALEA does not regulate encryption *per se*, but instead was adopted to maintain the *status quo* when it comes to interception of private communications.[1068] As such, it requires telecommunications service providers to be able to intercept communications carried out on their network and to make it available to law enforcement in its decrypted form, when served with the appropriate court order.[1069] This obligation only applies to encryption that has been applied by the provider itself, not by customers directly.[1070] Instant messaging platforms, such as *Facebook Messenger* and *WhatsApp* are excluded from CALEA's application,[1071] as well as email services, social networking platforms, and peer-to-peer services.[1072] However, services that are "substantial replacements for telephone services" (including VoIP) have been found to be subject to CALEA.[1073]

[1066] *Communications Assistance for Law Enforcement Act*, 47 (USC 2018).
[1067] Hurwitz, *supra* note 69 at 373.
[1068] *Ibid* at 381–382.
[1069] *Ibid* at 377.
[1070] Monique Mann, Angela Daly & Adam Molnar, "Regulatory arbitrage and transnational surveillance: Australia's extraterritorial assistance to access encrypted communications" (2020) 9:3 Internet Pol'y Rev 1 at 4.
[1071] Hurwitz, *supra* note 69 at 390.
[1072] Manpearl, *supra* note 2 at 71.
[1073] Hurwitz, *supra* note 69 at 388.

D) Decryption by TPDC of Data at Rest

CALEA does not apply to device manufacturers, even if they manufacture telecommunications equipment.[1074] For this reason, the government has relied on another act, the *All Writs Act* of 1789,[1075] when it comes to compelling a manufacturer to unlock a device.[1076] The application of this rather dated piece of legislation to such a novel issue has not been easy. Indeed, this has been met with strong opposition from TPDCs, including Apple, following the San Bernardino case.[1077] After Apple was compelled to unlock the suspect device in this case, the company appealed the decision on the basis that unlocking the device would pose too big a threat to data security.[1078] However, the appeal was never heard due to the fact that law enforcement was able to unlock the suspect's device with the assistance of a private company specialized in the circumvention of encryption methods.[1079] For this reason, it is uncertain if a TPDC could be compelled to unlock a device,[1080] especially considering TPDCs have now been implementing encryption in such way that they cannot themselves circumvent it.[1081] The standstill between the government and TPDCs in the United States demonstrates that alternative to backdoors must be found to address the "going dark" problem, as applied to data in transit.[1082]

[1074] Liguori, *supra* note 70 at 385.
[1075] *All Writs Act*, 28 USC 1651.
[1076] Hill-Smith, *supra* note 150 at 185.
[1077] *Ibid* at 187.
[1078] Tim Cook, "A Message to Our Customers", (16 February 2016), online: *Apple* <https://www.apple.com/customer-letter/>.
[1079] Hill-Smith, *supra* note 150 at 187.
[1080] *Ibid* at 187–188.
[1081] For example, Apple says it cannot extract data from an iPhone running iOS 8.0 or later. See Zarefsky, *supra* note 331 at 187.
[1082] See Chapter 8.

E) Lawful Hacking

"Lawful hacking,"[1083] or "police hacking"[1084] is the usage of techniques often employed by hackers by governments, in order to further their goals or detecting and preventing crimes, including circumventing encryption. Lawful hacking techniques can allow for (1) the capture of specific types of data; (2) the remote search of stored data; (3) the remote monitoring of computer use; (4) the interception of communications; (5) the remote activation of a suspect's webcam to proceed to visual observations; (6) and the remote deleting of unlawful data.[1085] As such, lawful hacking can serve both search and surveillance purposes.[1086]

The United States does not have a specific legislative instrument that regulates lawful hacking.[1087] However, rule 41(b)(6) of the *Federal Rules of Criminal Procedure* regulates remote access to computers via warrant.[1088] The rule has been used to deploy 'network investigative techniques' (NITs) in order to investigate crimes, regardless of the location of the device[1089] NITs can allow law enforcement to 'hack' the target's computer, with malware,[1090] by using either a vulnerability that already exists in the target's system, or by tricking the target into downloading infected software. The applicability of the Fourth Amendment to this investigate technique remains uncertain.[1091]

[1083] Eric Manpearl, "The International Front of the Going Dark Debate" (2018) 22:4 Va J L & Tech 158; Liguori, *supra* note 70.
[1084] Ivan Skorvanek et al, "'My Computer Is My Castle': New Privacy Frameworks to Regulate Police Hacking" (2019) 2019:4 BYU L Rev 997.
[1085] *Ibid* at 1009–1012.
[1086] *Ibid* at 1012.
[1087] Liguori, *supra* note 70 at 342.
[1088] *Ibid*.
[1089] Chen, *supra* note 3 at 189–190.
[1090] *Ibid* at 191.
[1091] Skorvanek et al, *supra* note 1084 at 1030.

NITs have been said to be an effective method law enforcement can use to circumvent encryption:

> Instead of encouraging system weaknesses through backdoors and dissuading the movement towards encryption, law enforcement can turn to NITs to take advantage of holes already present in the system. […] The spread of encryption will necessitate that law enforcement turn to hacking as an investigative tool in the future. Backdoors are increasingly no longer a viable option for agents to obtain access to devices, with or without a warrant. Consequently, tools like NITs will allow law enforcement to bypass encryption and features that anonymize users in an attempt to stave off the Going Dark phenomenon.[1092]

The evidence collected by law enforcement by using NITs can raise some issues when it comes to defendants' rights, mostly in regard to discovery and due process rights.[1093] Indeed, access to the full code of the NIT might be relevant for the defendant, but the government will usually resist disclosing the full code, as it could become a security issue.[1094] Regulation of the disclosure of vulnerabilities found by law enforcement to the public and industry actors following the use of NITs can be found in the *Vulnerabilities Equities Process*, an administrative tool.[1095]

6.3.2 The English Approach

The principle against self-incrimination in the UK can be abrogated by status, as it does not receive constitutional protection.[1096] As mentioned, this means that legislation can modify the

[1092] Chen, *supra* note 3 at 195.
[1093] *Ibid* at 195–196.
[1094] *Ibid* at 197–198.
[1095] Liguori, *supra* note 70 at 342.
[1096] Daniel Hochstrasser, "Encryption and the Privilege Against Self-Incrimination: What Happens When a Suspect Refuses to Divulge a Password" (2021) Forthcoming U New South Wales LJ at 15.

common law privilege against self-incrimination more easily than in the United States or in Canada. This is indeed the approach that was taken in the context of encryption, whether for data in transit or at rest.

A) Decryption by Suspect of Data at Rest

Section 49 of the *Regulation of Investigatory Powers Act 2000* (*RIPA*) allows for the compelled production of an encryption key, in specific circumstances.[1097] This power is strictly a decryption power, not a search or seizure power, as one of its requirements is that the ciphertext has previously been obtained in a lawful manner, either under a common law or a statutory power.[1098]

In order to impose such a disclosure requirement under s. 49 of *RIPA*, the officer that came to be in possession of the electronic device or data will need to obtain an authorization from an authorized official, [1099] before serving the notice upon the suspect. The suspect will then be given a reasonable amount of time to respond by handing over the plaintext of the data. Default to comply to the order can lead to prosecution, under s. 53 of *RIPA*.[1100] The suspect

[1097] *Regulation of Investigatory Powers Act 2000*, *supra* note 1012.
[1098] Palfreyman, *supra* note 7 at 364.
[1099] Namely, a "Circuit judge in England, a sheriff in Scotland or a County Court judge in Northern Ireland." However, some investigators will also be given a free-standing right to issue s. 49 notices, which means that prior judicial authorization will not always be required. See Bernard Keenan, "State access to encrypted data in the United Kingdom: The 'transparent' approach" (2020) 49:3–4 Common L World Rev 223 at 237.
[1100] Palfreyman, *supra* note 7 at 364–365, 368: "The punishment resulting from a conviction is up to two years of imprisonment, a fine, or both." An individual will only be declared guilty of this crime if the prosecution can prove beyond a reasonable doubt that that person was in possession of the encryption key.

will also be given the choice of turning in the encryption key, rather than producing the plaintext, as per s. 50 of *RIPA*.[1101]

The authorization will be issued if the authorizing official believes, on reasonable grounds:

> (a) that a key to the protected information is in the possession of any person,
>
> (b) that the imposition of a disclosure requirement in respect of the protected information is—
>
> > (i) necessary on grounds falling within subsection (3), or
> >
> > (ii) necessary for the purpose of securing the effective exercise or proper performance by any public authority of any statutory power or statutory duty,
>
> (c) that the imposition of such a requirement is proportionate to what is sought to be achieved by its imposition, and
>
> (d) that it is not reasonably practicable for the person with the appropriate permission to obtain possession of the protected information in an intelligible form without the giving of a notice under this section.[1102]

The requirement to believe on reasonable grounds that the suspect is in possession of the encryption key has been interpreted as being fairly easy to satisfy. In *Greater Manchester Police v Andrews*, the Court concluded that possession or ownership of the device permitted to draw the inference that the individual did indeed have knowledge of the encryption key.[1103] The proportionality requirement found in s. 49(2)(c) aims to balance the opposed interests at

---

[1101] *Regulation of Investigatory Powers Act 2000*, *supra* note 1012, s 50; Palfreyman, *supra* note 7 at 367. Law enforcement is also given the ability to compel the production of the key directly under s. 51 of *RIPA*, if it can satisfy more stringent requirements.
[1102] *Regulation of Investigatory Powers Act 2000*, *supra* note 1012, s 49(2).
[1103] *Greater Manchester Police v Andrews*, [2011] EWHC 1966 cited in Hochstrasser, *supra* note 1096 at 19.

play, including the privilege against self-incrimination.[1104] S. 49(2)d) basically ensures that this provision will only be used when no other method can easily allow law enforcement to access the plaintext, making s. 49 a "last resort."[1105] Under s. 49(3) of *RIPA*, compelled disclosure will be available under three circumstances:

> (a)in the interests of national security;
>
> (b)for the purpose of preventing or detecting crime; or
>
> (c)in the interests of the economic well-being of the United Kingdom.[1106]

The validity of this provision has been confirmed by the Court of Appeal for England and Wales in *R v S(F)*. The Court concluded that the independent existence of the encryption key made the privilege inapplicable and that in any case, a provision can indeed abrogate the privilege, as it is not an absolute right that must cede way to other imperatives in certain circumstances.[1107] As such, s. 49 of *RIPA* was found to be compatible with Article 6 of the *ECHR*.[1108] The Court however recognized that the suspect's knowledge of the encryption key may be incriminating, [1109] which is consistent with the American "act of production doctrine," as applied to encrypted data.

[1104] Keenan, *supra* note 1099 at 239, referring to the Court's interpretation of s. 49 in *Greater Manchester Police v Andrews*, *supra* note 1103.
[1105] Palfreyman, *supra* note 7 at 365. See also Keenan, *supra* note 1099 at 237.
[1106] *Regulation of Investigatory Powers Act 2000*, *supra* note 1012, s 49(3).
[1107] *R v S(F)*, [2009] 1 WLR 1489, cited in Hochstrasser, *supra* note 1096 at 16–18.
[1108] Hochstrasser, *supra* note 1096 at 17–18.
[1109] *Ibid* at 17; Keenan, *supra* note 1099 at 239. In this decision, the Court concluded that the privilege against self-incrimination is only triggered in relationship to the prove of ownership that comes from being able to decrypt the data or device. However, the encryption key in itself is not protected by the privilege because it exists separately from the defendant's will. As such, the privilege is only engaged when it comes to the act of decryption.

B) Decryption by TPDC of Data in Transit

The *Investigatory Powers Act 2016* (*IPA*)[1110] was adopted in response to the Snowden revelations and to various encryption cases emanating from the UK or from Europe.[1111] It provides law enforcement with the possibility of obtaining a 'technical capability notice' (TCN) under s. 253,[1112] which can be used to impose decryption obligations on a 'communications operator.'[1113] Section 253 works at two levels: first, by requiring that operators maintain the capacity to decrypt communications, and second, by removing encryption that the operator has itself applied, when it is reasonably practicable to do so.[1114] This provision is made applicable to operators located outside the UK.[1115] As will be examined in Chapter 8, this type of decryption power, imposed on TPDCs, should be avoided as they can unwittingly affect lawful users' security and privacy.

It remains unclear if the provision could prevent a TPDC from offering E2EE to their customers.[1116] It seems that 'over-the-top service providers' could be the object of a TCN, while free-standing encryption software providers would not.[1117]

[1110] *Investigatory Powers Act 2016*, *supra* note 1016.
[1111] Cian C Murphy, "The Crypto-Wars Myth: The reality of state access to encrypted communications" (2020) 49:3–4 Common L World Rev 245 at 247.
[1112] *Investigatory Powers Act 2016*, *supra* note 1016, s 253.
[1113] A "communications operator" includes 'telecommunications companies, internet service providers, email providers, social media platforms, cloud providers and other 'over-the-top services,' which are companies such as WhatsApp or Signal. See Mann, Daly & Molnar, *supra* note 1070 at 6.
[1114] *Ibid*.
[1115] *Investigatory Powers Act 2016*, *supra* note 1016, s 253(8); Keenan, *supra* note 1099 at 230.
[1116] Mann, Daly & Molnar, *supra* note 1070 at 7.
[1117] Keenan, *supra* note 1099 at 233–234.

C) Lawful Hacking Provisions

Section 99 of *IPA* allows law enforcement to obtain a specific warrant (namely an 'equipment interference' warrant) to use lawful hacking techniques *inter alia* to circumvent encryption, without compelling the suspect to produce the plaintext or the encryption key.[1118] Equipment interference warrants can be issued by a chief police officer and are subject to judicial oversight, except in urgent cases.[1119] Their use is limited to intelligence and security services in the UK.[1120]

With this authorization, law enforcement will be allowed to deploy malware on a suspect's devices, including to monitor the individual's communications.[1121] It can also be used to take control of the device remotely, to use a keystroke software, or to activate the device's webcam.[1122] TPDCs can also be compelled into providing assistance to law enforcement.[1123] It is important to note that the use of malware and other techniques does not guarantee that law enforcement will effectively be able to access the data it is looking for, as criminals will likely employ strong firewalls and sophisticated evasion techniques.[1124] Lawful hacking will be examined later on in this thesis and suggested as the best possible solution to the "going dark" problem, as applied to data in transit. It is also a potential alternative to compelled

[1118] Manpearl, *supra* note 1083 at 206.
[1119] Skorvanek et al, *supra* note 1084 at 1021.
[1120] Murphy, *supra* note 1111 at 251.
[1121] Skorvanek et al, *supra* note 1084 at 1022.
[1122] *Ibid*.
[1123] *Ibid* at 1021–1022.
[1124] Further, lawful hacking will often rely on the existence of a vulnerability in the software or hardware, which is not always present. See Rozenshtein, *supra* note 35 at 1206–1210.

decryption, in situations where the investigation requires the suspect to remain unaware of law enforcement's access to the data.

6.3.3 The Australian Approach

Australia's compelled decryption regime can be separated in two categories, depending on whether law enforcement is seeking to compel assistance from a suspect or from a TPDC. Generally speaking, Australia has been described as being on the forefront of advocacy against strong encryption in the world.[1125]

A) Power to Compel Suspects to Unlock Devices or Decrypt Data at Rest

Legislation at both the federal and state levels in Australia provide with court authorizations to compel the production of decrypted material or of encryption keys; some that may be available concomitantly with the application for a search warrant, some that can be obtained after the warrant has already been executed and electronic devices have been seized.[1126] For example, a s. 3LA warrant found in the *Crimes Act 1914* allows for compelled production when the magistrate is convinced that:

> (a) there are reasonable grounds for suspecting that evidential material is held in, or is accessible from, the computer or data storage device; and
> (b) the specified person is:
> (i) reasonably suspected of having committed the offence stated in the relevant warrant; or
> (ii) the owner or lessee of the computer or device; or
> (iii) an employee of the owner or lessee of the computer or device; or

[1125] Mann, Daly & Molnar, *supra* note 1070 at 2.
[1126] Hochstrasser, *supra* note 1096 at 25–26.

(iv) a person engaged under a contract for services by the owner or lessee of the computer or device; or

(v) a person who uses or has used the computer or device; or

(vi) a person who is or was a system administrator for the system including the computer or device; and

(c) the specified person has relevant knowledge of:

(i) the computer or device or a computer network of which the computer or device forms or formed a part; or

(ii) measures applied to protect data held in, or accessible from, the computer or device.[1127]

This provision poses a relatively low evidentiary burden to law enforcement when it comes to knowledge of the password, as possession of the device has been found to be sufficient, even when found in shared homes.[1128] The provision is applicable only to specific devices and does not provide law enforcement the power to compel production of encryption key or plaintext at large.[1129]

While these warrants have been found to implicate the principle against self-incrimination when it comes to alphanumeric passwords, Australia's absence of a bill of rights allows for the privilege to be abrogated by specific legislation, either explicitly or implicitly, making these provisions valid nonetheless.[1130] Courts have however determined that law enforcement officials lack the power to compel the production of an alphanumeric password at the time of arrest.[1131]

[1127] *Crimes Act 1914*, *supra* note 1022, s 3LA.
[1128] Hochstrasser, *supra* note 1096 at 34–35.
[1129] *Ibid* at 36.
[1130] *Ibid* at 26–27.
[1131] *R v Ford*, [2017] QSC 205, cited in Hochstrasser, *supra* note 1096 at 28–29.

In the absence of a specific court decision on the applicability of these principles to biometric encryption methods, it has been suggested that the privilege against self-incrimination is simply not applicable in this case, following an earlier decision from the High Court of Australia, which concluded that the privilege is not applicable to bodily evidence.[1132] In any case, whether the privilege against self-incrimination can be applied to biometric authentication measures or not is of little relevance, as legislation has indeed abrogated the privilege.[1133]

Two Australian states—Victoria and Queensland— have enacted human rights statutes that contain provisions granting individuals the right not to self-incriminate. Both these states have also passed legislation that allows for the compelled production of decrypted data or encryption keys.[1134] To determine if a provision that implicates the privilege is nonetheless valid, courts from these states use an analysis that focuses on finding the appropriate balance between the competing interests at play,[1135] which is strikingly similar to what is done in Canada. Under this analysis, it has been suggested that compelled production orders would likely be found to be valid in these states, as they provide law enforcement access to information of high importance, in a context where no other less intrusive mean can allow law enforcement to reach the same goal.[1136]

[1132] *Sorby v The Commonwealth*, (1983) 152 CLR 281 at 292, cited in Hochstrasser, *supra* note 1096 at 28.
[1133] Hochstrasser, *supra* note 1096 at 30–31.
[1134] *Ibid* at 31.
[1135] *Ibid* at 32.
[1136] *Ibid* at 33–34.

B) Power to Compel TPDCs to Unlock Devices or Decrypt Data (at Rest and in Transit)

Australia has also enacted a much-criticized piece of legislation that regulates encryption at the TPDCs level: The *Telecommunications and Other Legislation Amendment (Assistance and Access) Act* 2018 (*TOLA*).[1137] The overarching objective of this piece of legislation was "to introduce measures to better deal with the challenges posed by ubiquitous encryption."[1138] This act has been said to give free-reign to TPDCs to implement encryption measures as they see fit, while imposing "*ex post* decryption assistance obligations."[1139] It applies to various industry actors, including multinationals (such as Apple, Google, and Facebook), but also more generally virtually to any actor of the communications industry, including developers or suppliers of software, service providers, and entities that provides electronic services to more than one user in Australia.[1140]

Three specific instruments are now available to Australian law agencies that make it possible to obtain assistance from a communications provider: (1) a technical assistance request (TAR); (2) a technical assistance notice (TAN); and a technical capability notice (TCN). Compliance to a TAR is voluntary, while compliance to TANs and TCNs is mandatory.[1141] The distinction between the two provisions is that a TAN is applicable when the TPDC already has the ability to provide the type of assistance sought-after by law enforcement, while

[1137] Parliament of Australia, *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, *supra* note 1027.
[1138] Parliament of Australia, "Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Revised Explanatory Memorandum" (2018) at 2.
[1139] Peter Alexander Earls Davis, "Decrypting Australia's 'Anti-Encryption' legislation: The meaning and effect of the 'systemic weakness' limitation" (2022) 44 Computer L & Security Rev 1 at 3.
[1140] Nicola McGarrity & Keiran Hardy, "Digital surveillance and access to encrypted communications in Australia" (2020) 49:3–4 Common L World Rev 160 at 169–170.
[1141] Earls Davis, *supra* note 1139 at 4.

a TCN will require the TPDC to develop or implement this ability.[1142] The use of TANs and TCNs is limited to situations involving national security and the investigation of 'serious offences,' which is defined by *TOLA* as offences 'punishable by a maximum term of imprisonment of 3 years of more.'[1143] Both TARs and TANs are available without prior authorization by a judge or magistrate, but a TCN can only be issued by the attorney general, with approval from the communications minister.[1144] In any case, law enforcement will need to respect the applicable legal requirement to previously obtain the data or gain access to a device, as *TOLA* does not contain search and seizure powers.[1145]

TANs and TCNs can allow for various types of assistance, including "removing one or more forms of electronic protection (ie [sic] bypassing decryption)."[1146] These provisions can also be used to employ lawful hacking tactics, with the help of a TPDC.[1147] The specific technique contemplated by law enforcement with a TAN or TCN "must be reasonable, proportionate, practicable and technically feasible."[1148]

Section 317ZG of *TOLA* contains a specific provision that has been said to play "a pivotal role in establishing where the privacy/security balance"[1149] is, in relationship to the three abovementioned instruments. According to this provision, TPDCs retain the possibility to design their systems in whatever which way they desire and they cannot be compelled to

---

[1142] *Ibid*.
[1143] *Ibid*, referring to *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, *supra* note 1027, s 317B.
[1144] Stilgherrian, *supra* note 1033 at 2.
[1145] McGarrity & Hardy, *supra* note 1140 at 171.
[1146] *Ibid* at 170.
[1147] Earls Davis, *supra* note 1139 at 4.
[1148] McGarrity & Hardy, *supra* note 1140 at 171.
[1149] Earls Davis, *supra* note 1139 at 5.

implement or build a systemic weakness or vulnerability into their systems.[1150] In other words, TARs, TANs, and TCNs can only be used against specific devices, in specific investigations, not as a general way of lowering encryption standards throughout the country and the industry. As such, *TOLA* cannot be used to create a key escrow scheme (like what had been suggested in the 1990s in the United States) but can be used to exploit zero-day vulnerabilities in specific instances.[1151]

Further, s. 317T(4)(c)(i) of *TOLA* specifically prohibits the circumvention of encryption methods through a TCN when the TPDC lacks the technical ability to do so.[1152] Put differently, only a TAN can allow for compelled decryption by the TPDC, not a TCN. Section 317ZG(2) also provides a protection for encryption capabilities, as it prohibits the implementation of a system vulnerability that would impact encryption in a general sense, for example by requiring a TPDC to stop using end-to-end or full-disk encryption altogether.[1153] Similarly, s. 317ZG(3) of *TOLA* prohibits the systematic weakening of encryption, for example by imposing the use of short encryption key.[1154] Generally speaking then, *TOLA* does not aim to weaken or otherwise reduce encryption capacities in general; rather it aims to give law enforcement access to decrypted data in specific instances. The question that remains is if it is possible for TPDCs to comply with *TOLA* notices and circumvent encryption in specific cases, without impacting the strength of encryption at large.

[1150] *Ibid* at 10.
[1151] *Ibid* at 5.
[1152] *Ibid* at 12.
[1153] *Ibid*.
[1154] *Ibid* at 13.

Importantly, *TOLA* has possible extraterritorial effects, as its application is not limited to Australian investigations. On the contrary, the Australian government has expressly stated that the provisions are available to international partners, under Australia's mutual assistance framework.[1155] Further, the abovementioned provisions can be used against TPDCs that are not located in Australia, if its services are available within the country,[1156] making it a far-reaching provision considering the ubiquitous nature of the internet.

Australia's legislation on encryption found in *TOLA* has been said to be the broadest when compared to what is applicable in other *Five Eyes* countries, not only because it gives law enforcement the power to compel the "broadest category of providers and companies [and] to do the broadest category of assistance acts," but also because it provides with "the most broad and significant extraterritorial reach."[1157] By contrast, it has also been described as providing "the weakest oversight mechanisms and no protections for human rights,"[1158] which is especially worrisome due to the potential extraterritorial application of the provisions. This should be considered by Parliament when it comes to the enactment of compelled decryption or lawful hacking legislation in Canada.

[1155] Parliament of Australia, *supra* note 1138 at 2; McGarrity & Hardy, *supra* note 1140 at 176; Earls Davis, *supra* note 1139 at 4.
[1156] Earls Davis, *supra* note 1139 at 4; Mann, Daly & Molnar, *supra* note 1070 at 8.
[1157] Mann, Daly & Molnar, *supra* note 1070 at 11.
[1158] *Ibid*.

PART 2 – ACCESS TO DATA AT REST

CHAPTER 7 LAW ENFORCEMENT ACCESS TO ENCRYPTED OR OTHERWISE PROTECTED DATA DIRECTLY FROM SUSPECT

When law enforcement officials are facing a locked device or encrypted data, they can try different ways to gain access to the information that is relevant to their investigation. As referred to in the introduction to this thesis, Kerr and Schneier have regrouped the different options available to law enforcement into six categories of "encryption workarounds": (1) find the key; (2) guess the key; (3) compel the key; (4) exploit a flaw in the encryption scheme; (5) access plaintext when the device is in use; and (6) locate a plaintext copy.[1159] The applicability of a specific "workaround" is highly circumstantial and can also be limited by technical and logistical constraints that are placed on law enforcement.

The possibility of "finding the key"[1160] is contingent on the key being written down or stored in a way that is accessible to law enforcement, which will not always be the case.[1161] The same can be said of the option of "locating a plaintext copy," which will depend on the data being available from another location, often in the cloud.[1162] "Guessing the key" will depend on multiple factors, including the crucial factor of the length and strength of the key: the shorter and more obvious the key is, the more likely it will be possible for law enforcement

[1159] Kerr & Schneier, *supra* note 22.
[1160] The term "key" is used by Kerr and Schneier to encompass passcodes, passwords, and passphrases. *Ibid* at 996.
[1161] *Ibid* at 996–997. See for example *R v Nero*, 2016 ONCA 153, where the password was found written on a sticky note.
[1162] Sacharoff, *supra* note 20 at 220.

to guess it.[1163] If the user has used the same password for different online services, this can facilitate the guess.[1164] However, it can also be risky to use this technique, as some devices will delete the data contained on the device after a certain number of incorrect tries.[1165] A brute-force attack can also be used to "guess the key," but current encryption software can make this option obsolete,[1166] and it cannot be used to crack a biometric authentication method.[1167] Similarly, even if law enforcement guessed the key (or obtained it using another "workaround"), a hidden volume only accessible using a different password could remain inaccessible to law enforcement.[1168]

"Exploiting a flaw in the encryption scheme" entails using a weakness to gain access to the decrypted contents, which is a specific type of lawful hacking technique. While flaws in systems are not necessarily uncommon, they are usually fixed promptly by service providers after their discovery.[1169] The application of this "workaround" involves knowledge of the flaw and also considerable technological expertise,[1170] which some smaller law enforcement agencies may lack. Alternatively, law enforcement can outsource this "workaround," like

---

[1163] According to NordPass, a business offering password management services that use encryption, the world's most used password is still "123456," which takes less than one second to crack. "Top 200 most common passwords", (2022), online: *NordPass* <https://nordpass.com/most-common-passwords-list/>. However, short numeral passcodes (i.e., PINs) have been found to effectively protect devices from intrusion. See Carissa A Uresk, "Compelling Suspects to Unlock Their Phones: Recommendations for Prosecutors and Law Enforcement" (2021) 46:2 BYU L R 601 at 606–607.

[1164] Atwood, *supra* note 9 at 427.

[1165] See for example Darryl Boxberger, "How to have your iPhone erase all data after 10 failed passcode attempts in iOS 15", (4 March 2022), online: *Apple Insider* <https://appleinsider.com/articles/22/03/04/how-to-have-your-iphone-erase-all-data-after-10-failed-passcode-attempts-in-ios-15>.

[1166] Cohen & Park, *supra* note 3 at 172.

[1167] Uresk, *supra* note 1163 at 610.

[1168] Its actual existence would also remain unknown to law enforcement. See Vera Crypt, "Hidden Volume", online: *Vera Crypt* <https://veracrypt.eu/en/docs/hidden-volume/>. See also Cohen & Park, *supra* note 3 at 202–203; Atwood, *supra* note 9 at 425.

[1169] Kerr & Schneier, *supra* note 22 at 1006; Uresk, *supra* note 1163 at 608–609.

[1170] Kerr & Schneier, *supra* note 22 at 1006–1007.

what was done in the United States in the San Bernardino case. This was done at a very high cost however, restricting its application to a limited number of cases.[1171]

The possibility of "accessing the device while it is in use" is twofold: first, law enforcement can gain remote access to the device by using lawful hacking techniques; or second, law enforcement can gain access to the physical device while it is in a decrypted state, at the time of arrest for example.[1172] Lawful hacking techniques are very promising when it comes to the circumvention of encryption by law enforcement but, once again, their concrete application depends on multiple factors, including the level of complexity of the encryption system used and the level of sophistication of suspects themselves. Lawful hacking also requires technical expertise that may be out of reach of some law enforcement agencies.

The fastest way of accessing the data will be, in most cases, to compel the owner of the device to unlock it and grant law enforcement access to its data,[1173] unless the suspect voluntarily agrees to unlock it or to reveal their password. [1174] This will also be the "workaround" that uses the least technical knowledge, as well as requiring virtually no additional financial

[1171] Mark Hosenball, "FBI paid under $1 million to unlock San Bernardino iPhone: sources", *Reuters* (4 May 2016), online: <https://www.reuters.com/article/us-apple-encryption/fbi-paid-under-1-million-to-unlock-san-bernardino-iphone-sources-idUSKCN0XQ032>. Law enforcement can now also purchase the software directly from such company, with prices estimated between 2 499$ to 30 000$, depending on the specific software. See Uresk, *supra* note 1163 at 607–608.

[1172] Kerr & Schneier, *supra* note 22 at 1007–1008.

[1173] The data might be stored directly on the device or be made accessible remotely, using cloud computing.

[1174] See *inter alia R v SL*, 2019 ONCJ 101 (consent to verbally reveal password found to be valid); *R v Hiscock*, [2016] CanLII 96899 (consent to verbally reveal password found to be invalid); *R v Smith, Wynter*, 2017 ONSC 4683 (consent to unlock phone using thumbprint found to be invalid); *R v Boutros*, 2018 ONCA 375 (breach of s. 10[b] of the *Charter* linked to law enforcement requesting the suspect to provide the password to his cellphone); *R v Azonwanna*, 2020 ONSC 5416 (breach of s. 10[b] of the *Charter* linked to law enforcement request to unlock cellphone. It should be noted however that in this case the Court determined that asking a suspect for a password is not a consent search *per se*, although it raises similar considerations); *R v Subia*, 2021 ONSC 6628 (consent to verbally reveal password found to be valid).

resources to be expended. Put differently, compelled decryption is the simplest solution to the encryption problem.[1175] Conversely, "[c]ompelled decryption is the most important self-incrimination issue of the digital age."[1176]

As it currently stands, Canada's law enforcement lacks a specific power to compel suspects to unlock devices or decrypt data.[1177] Indeed, lower courts have made it clear that an individual cannot be forced to reveal an alphanumeric password[1178] or a swipe pattern used to unlock a phone.[1179] Similarly, it has been decided that an impression warrant (s. 487.092 of the *Criminal Code*) cannot be used to force a suspect to unlock a phone using a fingerprint.[1180] The current non-availability of this "workaround" raises an important question: should compelled decryption powers be available to law enforcement officials in Canada? If so, under what framework?

Unlike other tools that are used by criminals, encryption has multiple positive applications for society and should be protected, not weakened. Encryption is not only used by criminals to hide their doings but is now mainstream,[1181] in a world where individuals tend to lose faith in the idea that online privacy can exist. As such, it is one of the last ramparts of digital privacy

[1175] Uresk, *supra* note 1163 at 605.
[1176] David Rassoul Rangaviz, "Compelled Decryption & State Constitutional Protection Against Self-Incrimination" (2020) 57:1 Am Crim L Rev 157 at 157.
[1177] Diab, *supra* note 3 at 276; Dheri & Cobey, *supra* note 77 at 20; Gill, Israel & Parsons, *supra* note 3 at 65; Public Safety Canada, *supra* note 79 at 61.
[1178] *R c Boudreau-Fontaine*, *supra* note 779; *R v Shergill*, *supra* note 230.
[1179] *R v Talbot*, 2017 ONCJ 814.
[1180] *Impression Warrant Application (Re)*, 2016 ONCJ 197. However, the suggestion from the CACP that the general warrant provision (s. 487.01 of the *Criminal Code*) could be used in this manner does not seem to have been examined by a Court in a published decision. See Canadian Association of Chiefs of Police, *supra* note 87.
[1181] Cohen & Park, *supra* note 3 at 171.

This must be part of the discussion when it comes to compelled decryption and other methods to access decrypted data.

Accordingly, this chapter will address the possibility of law enforcement being permitted to compel a suspect to unlock a device that uses either biometric authentication methods or alphanumeric passwords. It will start by suggesting an approach that reunifies the principle against self-incrimination and the protection against unreasonable search and seizure and will apply this approach to the subject of compelled decryption and unlocking of devices. It will then continue on to demonstrate that current provisions in the *Criminal Code* and current common law powers cannot effectively authorize such power.

Ultimately, this will lead to a concrete proposal of what compelled decryption and unlocking of devices should look like in Canada, in order to minimally respect ss. 7 and 8 of the *Charter* and adequately balance the opposed interests at play. The consequences of refusing to unlock a device will also be examined,[1182] as well as the implications regarding the right to remain silent and its positive obligations on police officers.[1183] The potential application of s. 1 of the *Charter* will finally be examined, to account for the possibility that the suggested framework could be considered as infringing the *Charter*.

The term "minimally" used in the last paragraph warrants some additional comments. The *Charter*, as part of Canada's Constitution, needs to be respected at all times when the state is interacting with its citizens. This is uncontroversial to say the least. However, it must be kept

[1182] Such as charges of contempt or failing to follow a valid law enforcement order. See Kerr & Schneier, *supra* note 22 at 1005.

[1183] For example, in *R v Harder*, 2017 ONCJ 280 at para 33, it was decided that the police officer had threatened the accused, thus infringing his *Charter* rights, when he stated that they could break the accused's phone if he did not provide them with the password.

in mind that while the *Charter* does create obligations for the state, it only prescribes the lower limit of what is acceptable when the state is interacting with its citizens. In other words, the *Charter* does not necessarily provide the *best* or *most optimal* solution to a question that involves protected rights and freedoms but provides a starting point that can be improved upon—a protection that can be enhanced—if Parliament decides to do so.

The framework suggested in this thesis will accordingly set up what would minimally need to be respected in order for compelled decryption to be found to respect both ss. 7 and 8 of the *Charter*. While some comments on the additional requirements that could be imposed by Parliament will be made along the way,[1184] it should be kept in mind that Parliament could indeed determine that compelled decryption is simply not something that it wants to endorse at all. That would evidently respect the *Charter*, by not only respecting the minimum guarantee that will be described hereinafter but also going above and beyond that requirement.

This section only considers data at rest, which is data in storage on a device or on a cloud that is accessible from the device. Data in transit will be considered subsequently in Part 3. The possibility of compelling assistance from a TPDC will be examined in Chapter 8.

7.1 The [Missing] Link Between the Principle Against Self-Incrimination and the Protection Against Unreasonable Search and Seizure

The principle against self-incrimination and the protection against unreasonable search and seizure are usually perceived as being two separate entities that do not interact with each other; they are on different tracks that will never meet. One is seen as protecting against

[1184] See *inter alia* Section 7.3.1(A) and (B)(i) *infra*

compulsion, while the other protects against *intrusion*.[1185] However, the protections bestowed by ss. 7 and 8 of the *Charter* can—and should—be reconciled in order to properly address the unique concerns that arise in the context of compelled decryption and unlocking of devices.

Encryption, whether at the disk, file, or device level, whether applied to data at rest or data in transit,[1186] restricts access to data that can be relevant to an investigation, effectively preventing the state from accessing the information pertinent to a specific case. Concretely, law enforcement officials will be able to seize a device or intercept the communication, while potentially respecting s. 8 of the *Charter*, but will not be able to search the device or access the contents of the communication, all because of encryption technologies. This is where ss. 7 and 8 get intertwined: in some cases, the only way to access the plaintext (i.e., data in its decrypted and readable form) obtained by constitutionally valid *intrusion* will be by using *compulsion* against a suspect.[1187] In these situations, without the interplay of self-incrimination, search and seizure becomes obsolete; the state is left with a metal box or an undecipherable ciphertext, deprived of all meaning.

American scholar Laurent Sacharoff has suggested that encryption requires us to find a way to reunite or harmonize the constitutional protections given to self-incrimination and against unreasonable search and seizure.[1188] Bryan H. Choi suggested a similar approach,[1189] as well

---

[1185] Or as Richard A. Nagareda puts it regarding the American context, "the Fifth Amendment addresses the 'giving' of evidence by a suspect; the Fourth, the 'taking' of evidence by law enforcement." See Richard A Nagareda, "Compulsion 'To Be a Witness' and the Resurrection of Boyd" (1999) 74 NYU L Rev 1575, as cited in Sacharoff, *supra* note 20 at 205. See also Brejt, *supra* note 948 at 1188.

[1186] See Chapter 2.

[1187] See *inter alia* Cole, *supra* note 213 at 179, who recognizes that compelled decryption raises both self-incrimination and unreasonable search and seizure considerations.

[1188] Sacharoff, *supra* note 20.

[1189] Choi, *supra* note 537.

as other authors.[1190] To do so, Sacharoff and Choi both suggest a focus on the values that the Fourth and the Fifth Amendments share, rather than on the terrains they traditionally have been confined to.[1191] While formulated for American criminal law, this approach can be adapted to fit the Canadian experience with self-incrimination and search and seizure principles. [1192] Besides, the SCC has recognized that particular circumstances can indeed require that both provisions be considered alongside one another.[1193]

7.1.1 The Shared Values of ss. 7 and 8 of the Charter

A) Restricting State Power / Promoting Privacy

> *Ultimately, the joint purpose of the two [provisions] is to set strong default presumptions against the arbitrary exercise of government power.*[1194]

Sections 7 and 8 of the *Charter*, like their American counterparts in the Fourth and Fifth Amendments, aim to limit the state's power to intrude into the lives of citizens.[1195] Specifically, the provisions seek to regulate the collection of information by the government in the context of criminal prosecutions.[1196] The limitations that s. 8 of the *Charter* imposes on law enforcement are fairly evident: law enforcement's ability to intrude upon someone's

---

[1190] See for example Abbey Flynn, "Physical Fruits vs. Digital Fruits: Why Patane Should Not Apply to the Contents of Digital Devices" (2021) 2021:1 U Ill JL Tech & Pol'y 1.
[1191] Sacharoff, *supra* note 20 at 206; Choi, *supra* note 537 at 193.
[1192] It should be noted that not all scholars agree with the need to harmonize both protections. See for example, Brejt, *supra* note 948. However, Brejt's analysis still aims to give full effect to both provisions, which is the same goal shared by Sacharoff and Choi. The method used to reach that goal may be different, but in the end, Brejt also advocates for recognizing the important place of self-incrimination when it comes to compelled decryption.
[1193] *Jones II*, *supra* note 249 at paras 30–31.
[1194] Choi, *supra* note 537 at 194.
[1195] Conroy & Scassa, *supra* note 257 at 116; Metz, *supra* note 936 at 434.
[1196] Flynn, *supra* note 1190 at 7.

reasonable expectation of privacy depends on the existence of a warrantless search or seizure power, or upon the obtention of a judicial authorization.[1197] Any other intrusion will be deemed unreasonable and contrary to the *Charter*.[1198] Further. s. 8 of the *Charter* does not itself confer a power to law enforcement to conduct "reasonable" search and seizure.[1199] Law enforcement officials must find the source of their search or seizure power somewhere else, either in the *Criminal Code* or in the common law.

In the context of self-incrimination, the SCC has recognized that s. 7 also aims to protect against the risk that law enforcement officials will abuse their power.[1200] The various rules that emanate from the overarching principle against self-incrimination exemplify how state power is limited by self-incrimination considerations. For example, the right to counsel will prohibit law enforcement from questioning a suspect before they have the occasion to speak with a lawyer of their choice. Concretely, then, as with all the legal rights found within the *Charter*, neither provision grants powers to law enforcement; rather they limit what law enforcement officials can do when interacting with a suspect or an accused individual.

In *Hunter*, the SCC left the door open for s. 8 to be conceived as promoting interests other than privacy.[1201] Explicitly in *R v SAB*, Justice Arbour recognized that s. 8 could also allow for self-incrimination to be considered under the principle against unreasonable search and

---

[1197] *Jarvis II*, *supra* note 263 at para 99.
[1198] See generally Chapter 5.
[1199] *Hunter*, *supra* note 31 at 157–158.
[1200] What Penney calls the "abuse-prevention rationale." 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" (2003) 48 Crim LQ 249 at 250. See also Dufraimont, *supra* note 344 at para 15; John Henry Wigmore, *Principles of judicial proof, as given by logic, psychology, and general experience, and illustrated in judicial trials* (Boston: Little, 1913) cited in *Dubois*, *supra* note 360 at 358; *Hart*, *supra* note 379 at para 123; *Jones I*, *supra* note 343 at 250; Choi, *supra* note 537 at 193.
[1201] *Hunter*, *supra* note 31 at 159.

seizure.[1202] On the other side, it has been implied that s. 7 contains a residual protection for privacy.[1203] For Penney, both the "abuse-prevention rationale" and the "free choice rationale"[1204] that can be used to justify self-incrimination provisions implicate privacy considerations.[1205] Accordingly, both ss. 7 and 8 of the *Charter* provide privacy protections, albeit in different ways and at different levels.

In the context of American criminal law, Sacharoff writes that the Fifth Amendment can be interpreted as protecting privacy indirectly when it comes to passwords. In his own words: "we may view the Fifth Amendment as protecting the privacy of papers that current Fourth Amendment case law has wrongly failed to protect. Or, put another way, we can simply say that the Fifth Amendment protection for passwords furthers Fourth Amendment goals of privacy."[1206] The Fifth Amendment then, as does s. 7 of the *Charter*, "generates privacy spillovers,"[1207] and the Fourth Amendment should not "bear the full weight of privacy."[1208] In a context where privacy is seriously undermined by the ease with which law enforcement can access personal data, encryption promotes privacy by posing barriers to law enforcement.[1209] As both provisions seek to protect privacy, an analysis of compelled

[1202] *SAB*, *supra* note 430 at paras 35–36.
[1203] *BC Securities*, *supra* note 376 at para 68; *Beare*, *supra* note 681 at 412; *R v O'Connor*, *supra* note 304 at paras 110–113; Benoît Pelletier, "La protection de la vie privée au Canada" (2001) 35 RJT 485–522 at para 49; Dalla Guarda, *supra* note 32 at 127.
[1204] Which is the theory that "criminal suspects should, as a matter of principle, have a certain measure of freedom to choose whether to provide self-incriminating evidence to the state." Penney, *supra* note 1200 at 250.
[1205] *Ibid* at 263–264. See also *Thomson Newspapers Ltd v Canada*, *supra* note 345 at 480.
[1206] Sacharoff, *supra* note 20 at 243.
[1207] Choi, *supra* note 537 at 191. See also Lemus, *supra* note 220 at 557; Redfern, *supra* note 215 at 609.
[1208] Choi, *supra* note 537 at 192.
[1209] In other words, encryption is directly related to privacy because it enforces control over private information. See Lemus, *supra* note 220 at 559.

decryption can only be satisfactory when both protections are reconciled in accordance with the objectives they seek to promote.

The protection against unreasonable search and seizure has been criticized for not affording strong privacy protection to individuals, mainly because of the ease with which law enforcement can obtain warrants that can give them access to a person's devices and virtually all the data they contain or give access to.[1210] As such, s. 8 of the *Charter* can be perceived as doing little to restrict state power and adequately balance the opposed interests at play when it comes to personal data. Allowing law enforcement to compel individuals to unlock their devices without obtaining judicial authorization would effectively annihilate the remainder of the privacy protections individuals have towards their electronic devices and the data they contain, without leaving room for any considerations related to self-incrimination.

B) Truth-Seeking Function

Generally speaking, adversarial justice systems allow for more values to compete when crafting criminal procedure rules, as opposed to inquisitorial systems that will give more weight to the search for truth as the central value of their system.[1211] However, this does not mean that the search for the truth of a case is not important in Canadian criminal procedure.[1212] Search and seizure powers can be seen as tools that allow law enforcement to get as close to

[1210] Sacharoff, *supra* note 20 at 214.
[1211] Damaska, *supra* note 306 at 579; Jackson, *supra* note 306 at 504.
[1212] As stated by the SCC in *R v Handy*, 2002 SCC 56, [2002] 2 SCR 908 at para 44: "[t]he criminal trial is, after all, about the search for truth as well as fairness to an accused." See also *S (RJ)*, *supra* note 343 at para 156, in which Iacobucci J. (writing for the majority) recognized the importance of the truth-seeking goal of the criminal process.

the truth of a case as possible, by allowing officers to collect as much relevant evidence as possible.

The Canadian experience with self-incrimination also considers the search for truth as a value it seeks to promote, as the privilege against self-incrimination operates by way of immunities in Canada. Rather than granting a general right to refuse to answer questions to witnesses (including an accused)—as was done at common law and is still done in the United States—testimonial privileges promote the truth-seeking function of the criminal process by ensuring that the trier of fact will be presented with, once again, as much relevant evidence as possible. The fact that the protection against self-incrimination seeks to eliminate untrustworthy evidence also promotes the search for truth in the criminal process.[1213] However, it must be kept in mind that the principle against self-incrimination can indirectly produce the consequence that relevant material will be excluded from the inquiry.[1214] The fact that the principle against self-incrimination can sometimes compete with the truth-seeking function of the criminal process was explicitly recognized by the dissenting judges in *Nedelcu*.[1215]

7.1.2 The Common Method Emerging From ss. 7 and 8 of the Charter*: A Focus on Reasonableness*

The Supreme Court of the United States had originally recognized in *Boyd v United States* that the Fourth and the Fifth Amendment should be read together, as doing the opposite would

[1213] Penney, *supra* note 1200 at 253.

[1214] Most importantly, the right to remain silent and the right of the accused not to be compelled as a witness, both derived from the principle against self-incrimination, will indeed have for effect that relevant information will remain unknown for the trier of facts, thus doing the opposite of promoting the truth-seeking function of the criminal process. The confessions rule is also more concerned with other considerations than with the search for truth. See *Hodgson*, *supra* note 499 at 465.

[1215] *Nedelcu*, *supra* note 393 at 119 [as per LeBel J. dissenting reasons].

unduly restrict the Amendments from serving their function and reaching their full potential.[1216] However, subsequent interpretation of the Amendments and of *Boyd* did not follow this vision, on the tenet that it created a immunity that was overly broad, which would obstruct law enforcement in their valid efforts to investigate and prosecute crimes.[1217] The reconciliation of both Amendments that emanates from *Boyd* was potentially too ahead of its time.[1218] When applied to the Canadian experience with self-incrimination, however, the idea of reconciling the two protections does not create too broad an immunity or sphere of privacy. Both provisions allow for intrusion into a protected interest under s. 7 or a privacy interest under s. 8, as long as it is done in a reasonable manner.

Both the principle against self-incrimination and the protection against unreasonable search and seizure aim to balance competing interests.[1219] As seen in Chapter 3, criminal law is very much aware and used to this tension between law enforcement's legitimate need and citizens' interests, but, in the context of encryption, the tensions at play seem even more evident, not least because encryption transforms information that would normally have been within the scope of law enforcement's grasp into information that is out of their reach. In other words, encryption shifts the equilibrium between the state and the individual that existed prior to the advent of this technology.[1220]

[1216] *Boyd v United States*, 1886 US 616.
[1217] Choi, *supra* note 537 at 190. See also Sacharoff, *supra* note 20; Flynn, *supra* note 1190 at 8.
[1218] Choi, *supra* note 537 at 192–193.
[1219] *Thomson Newspapers Ltd v Canada*, *supra* note 345 at 539; *Hunter*, *supra* note 31 at 156–157.
[1220] As Dan Terzian puts it: "Prior to decryption, the government obtained a warrant and got the sought data. Even if the sought documents were held in a safe and the government lacked the combination, the government still obtained them because it could crack the safe. [...] But if the data lies on an encrypted device, equilibrium is disrupted." See Dan Terzian, "Forced Decryption as Equilibrium - Why It's Constitutional and How Riley Matters" (2015) 109:4 Northwest U L Rev 1131 at 1139.

The method ss. 7 and 8 share to attain the goal of striking the appropriate balance between opposed interests focuses on what is *reasonable*, conceived broadly. On one side, section 8 uses reasonableness *directly* at two levels: (1) to determine if the individual claiming protection has a *reasonable* expectation of privacy in the subject matter of the search; and (2) to determine if that search or seizure was *reasonable*, under the *Collins* test.[1221] On both levels, the determination of what is reasonable entails an assessment into what Canadians have come to expect with regards to their privacy and is laden with normative considerations and reflections.

On the other side, section 7 uses reasonableness *indirectly*, when it comes to the determination of what is acceptable under the principles of fundamental justice, as it seeks to find a balance between individuals rights, including the right against self-incrimination, and societal rights. As the SCC specified in *Thomson*, the determination of the scope of a principle of fundamental justice entails finding the "just accommodation between the interests of the individual and those of the state."[1222] The principle against self-incrimination, as a principle of fundamental justice, is not a "free-standing right,"[1223] which means it will need to be interpreted in light of other interests. As such, specific rules or provisions that implicate the principle against self-incrimination will not automatically contravene s. 7 of the *Charter*, as the component rights of s. 7 can be limited, in accordance with the principles of fundamental justice. In other words, the determination of the scope of the principle against self-

[1221] *R v Collins*, *supra* note 31.
[1222] *Thomson Newspapers Ltd v Canada*, *supra* note 345 at 539. See also Dalla Guarda, *supra* note 32 at 127; Ungberg, *supra* note 38 at 553.
[1223] *S (RJ)*, *supra* note 343 at para 100.

incrimination then involves assessing what is *reasonable*, in our society and in the current day and age.[1224]

Another way to reframe this interplay can be found in a statement made by the SCC in *Mills I*: "a reasonable search or seizure is consistent with the principles of fundamental justice."[1225] The reasonableness aspect of s. 8 is consequently strongly linked to the principles of fundamental justice found under s. 7 of the *Charter*, and therefore to self-incrimination indirectly. Consequently, a framework allowing law enforcement to compel individuals to decrypt their data or unlock their devices will respect ss. 7 and 8 of the *Charter* if it is *reasonable*, with regards to the entirety of the circumstances.

The remainder of this chapter will examine all the different steps necessary in order to indeed craft a framework that respects the imperatives prioritized under ss. 7 and 8 of the *Charter*, in order to properly balance the legitimate interests of law enforcement with valid privacy and self-incrimination considerations that citizens may have, in the specific context of encryption of digital devices.

7.2 A Reunified Protection Against Compelled Decryption of Data and Unlocking of Devices under ss. 7 and 8 of the Charter

In general, the principle against self-incrimination protects from compelled testimony that tends to incriminate the witness, whether at trial or in the pretrial phase of the criminal process. The SCC has, however, recognized that the principle against self-incrimination can afford

[1224] Like the protection against unreasonable search or seizure, the principle against self-incrimination then allows for a normative dimension to be considered. See Dufraimont, *supra* note 344 at para 16.
[1225] *Mills I*, *supra* note 431 at para 88.

some degree of protection to both testimonial evidence and non-testimonial (real) evidence,[1226] though it has shown a clear preference for analyzing non-testimonial evidence issues under s. 8 of the *Charter*.[1227]

One of the difficulties of finding consensus in the context of compelled decryption is that the lines between testimonial and material evidence become blurred by this technology: the act of decryption carries testimonial characteristics, while the encrypted data that is sought by law enforcement is real evidence.[1228] Further, it can be argued that encryption keys, while sometimes using alphanumeric language, are more akin to a mechanical lock, thus closer to real evidence,[1229] even though the disclosure of keys is testimonial. This dichotomy is one of the reasons why the principle against self-incrimination must be reconciled with the protection against unreasonable search and seizure in the context of compelled decryption.

For these reasons, and in order to harmonize both provisions, the consequences of the **act of decryption** are more suitable to an analysis under s. 7, while the privacy aspects linked to the **encrypted data** should be analyzed under s. 8 of the *Charter*. Together, the conclusions that will emanate from the analysis conducted here will provide insight into the possibility of creating a compelled decryption scheme that respects the imperatives put forth by the *Charter*.

Before commencing, it is useful to summarize the results of the analysis up front. It will be suggested below that compelled decryption creates a deprivation of the liberty interest of

---

[1226] *Stillman*, *supra* note 353; *SAB*, *supra* note 430 at paras 34–35; *R v Collins*, *supra* note 31 at 284; Dalla Guarda, *supra* note 32 at 134.
[1227] Penney & Gibbs, *supra* note 3 at 232; referring to *SAB*, *supra* note 430.
[1228] Ungberg, *supra* note 38 at 554; Lemus, *supra* note 220 at 547, 555; Vivek Mohan & John Willasenor, "Decrypting the Fifth Amendment: The Limits of Self-Incrimination in the Digital Era" (2012) 15 U Pa J Const L Height Scrutiny 11 at 12.
[1229] Penney & Gibbs, *supra* note 3 at 233. See also *inter alia* Opderbeck, *supra* note 6 at 910.

individuals under s. 7 and implicates the privacy interests protected by s. 8. However, it is submitted that a legislative framework on compelled decryption can be crafted that will both be in accordance with the principles of fundamental justice under s. 7 and that will allow for reasonable searches or seizures under s. 8 of the *Charter*. Accordingly, in order to respect both provisions, a legislative scheme specifically applicable to compelled decryption—that imposes stringent conditions on law enforcement and grants immunity to the suspect—would need to be adopted by Parliament.[1230] In the absence of such scheme currently applicable in Canada, it will be argued that law enforcement presently lacks the power to impose decryption obligations upon Canadians and that any occurrence of compelled decryption effectively violates ss. 7 and 8 of the *Charter*, regardless of the encryption mechanism used (biometric, alphanumeric, or other).[1231]

7.2.1 Section 7 Considerations Towards the Act of Decryption

In *White*, the SCC summarized the three-step approach to determine whether s. 7 is infringed:

> The first question to be resolved is whether there exists a real or imminent deprivation of life, liberty, security of the person, or a combination of these interests. The second stage involves identifying and defining the relevant principle or principles of fundamental justice. Finally, it must be determined whether the deprivation has occurred in accordance with the relevant principle or principles: see *R. v. S. (R.J.)*, [1995] 1 S.C.R. 451, at p. 479, *per* Iacobucci J. Where a deprivation of life, liberty, or security of the person has occurred or will imminently occur in a manner which does

[1230] Again, Parliament could decide to go further than these suggestions, but could not go below them. See *supra* at the beginning of this chapter.

[1231] As such, consent to decrypt from the suspect would be essential. See for example, *Borden*, *supra* note 848 at 159.

> not accord with the principles of fundamental justice, a s. 7 infringement is made out.[1232]

Accordingly, this approach will be followed *infra* to determine whether compelled decryption has the potential to infringe s. 7 of the *Charter*.

An important caveat must be noted here. As examined in Chapter 4, self-incrimination is not only considered under s. 7 of the *Charter* but also in related rules that are found elsewhere in the *Charter* and in common law rules. A decision was made here to focus the analysis on the impact of compelled decryption on s. 7 of the *Charter* for two reasons. First, the right to silence and the right to counsel, while important protections against coerced self-incrimination, do not directly come into play when it comes to compelled decryption done with a judicial authorization. As this thesis will contend that compelled decryption can only be justified under s. 7 of the *Charter* in presence of a judicial authorization, these rights will only have a limited impact on the analysis suggested hereinafter. However, it should be clear that compelled decryption done without a judicial authorization would not only contravene the principle against self-incrimination, but also be a breach of the more specific right to silence, under s. 7 the *Charter*.[1233] Further, compelled decryption done without allowing the opportunity to consult with counsel, if this right is affirmed by the suspect, would also be a breach of s. 10(b) of the *Charter*.

Second, use and derivative use immunity, provided by ss. 7 and 13 of the *Charter*, were examined in Chapter 4 to demonstrate that immunities can be used to alleviate the impact of self-incrimination on individuals. These embodiments of the principle against self-

[1232] *White*, *supra* note 388 at para 38.
[1233] Alongside a s. 8 of the *Charter* violation, which will be examined *infra*.

incrimination apply to the trial phase of the criminal process, not the pre-trial phase where compelled decryption stands. As such, s. 13 does not provide motives to prohibit compelled decryption in the first place but provides insight into how immunities can be used to create a framework that respects the overarching protection against self-incrimination. Nonetheless, it will become clear that compelled decryption, without some type of correlative immunity, should be prohibited under s. 7 of the *Charter*.

A) Risk of Real or Imminent Deprivation of Life, Liberty, Security of the Person, or a Combination of these Interests

The obligation to unlock a device or decrypt data directly involves the liberty interest of s. 7 of the *Charter*, as individuals under investigation will face prosecution—and potentially imprisonment—following the possible discovery of evidence or illegal material on their devices. If a compelled decryption scheme was adopted, individuals could also risk imprisonment for contempt following a refusal to decrypt their devices or data. In a sense, this is very similar to the obligation to appear for fingerprinting prior to conviction under the *Identification of Criminals Act*, which the SCC determined implicated the rights guaranteed by s. 7 "because they require a person to appear at a specific time and place and oblige that person to go through an identification process on pain of imprisonment for failure to comply."[1234] It also resembles the regulatory regimes that compel people to make statements, such as the one examined by the SCC in *White*.[1235]

[1234] *Beare*, *supra* note 681 at para 29.
[1235] *White*, *supra* note 388.

The coercion that comes from this act also involves the liberty interest found in s. 7, as the individual subjected to this obligation would lose "a degree of autonomy in making decisions of fundamental personal importance,"[1236] that is the decision to collaborate or not with the authorities in the course of a criminal investigation that concerns them.

B) Identification of the Relevant Principle of Fundamental Justice

First and foremost, compelled decryption triggers the protection against self-incrimination because of the testimonial self-incriminating aspects of the act of decryption. This is consistent with the recognition by the SCC that the act of producing evidence can carry communicative meaning that triggers the protection against self-incrimination,[1237] and with the American experience with compelled decryption, where most courts have recognized the testimonial nature of decryption.[1238] As stated by Penney and Gibbs, the act of decryption indeed carries an intrinsic incriminating potential, due to the fact that the ability to decrypt is an express assertion of possession and control of the device or data by the individual, and thus

[1236] *Morgentaler v R*, [1988] 1 SCR 30 at 166. See also *B (R) v Children's Aid Society of Metropolitan Toronto*, [1995] 1 SCR 315 at 368 in which the Court stated that "… liberty does not mean mere freedom from physical restraint. In a free and democratic society, the individual must be left room for personal autonomy to live his or her own life and to make decisions that are of fundamental personal importance."
[1237] *BC Securities*, *supra* note 376 at para 47.
[1238] See Section 6.3.1 *supra*.

provides evidence of that.[1239] This has been accepted by some American courts.[1240] The act of decryption can also communicate authenticity (i.e., decryption recognizes the password or biometric key as being authentic) and can be used as evidence of authenticity by the Crown.[1241] Specifically in the context of social media, being compelled to give law enforcement access to a profile implicitly recognizes ownership of the profile and potentially the authenticity of the evidence related to that profile.[1242] This is consistent with the definition given to incrimination in *Nedelcu*, as the act of decryption could be used by the prosecution in a case to prove guilt.[1243]

Additionally, when it comes to compelled decryption of a device using a fingerprint, compelled decryption also involves the choice of what finger to use,[1244] which also carries testimonial significance, namely that the individual knew what finger to use, and thus is likely to be the owner of the device. Biometric features allow for a particularly strong inference of ownership of the device, as physical features cannot be shared, unlike passwords.[1245]

[1239] See also Adam M Geshowitz, "Password Protected - Can a Password Save Your Cell Phone from a Search Incident to Arrest" (2011) 96 Iowa L Rev 1125 at 1171–1172; Joshua A Engel, "Rethinking the Application of the Fifth Amendment to Passwords and Encryption in the Age of Cloud Computing" (2012) 33:3 Whittier L Rev 543 at 552; Goldman, *supra* note 211 at 227; Jarone, *supra* note 46 at 790; Madeline Leamon, "Unlocking the Right against Self-Incrimination: A Predictive Analysis of 21st Century Fifth Amendment Jurisprudence" (2019) 64:2 Wayne L Rev 583 at 597; Metz, *supra* note 936 at 454; Redfern, *supra* note 215 at 626–627; Nathan Reitinger, "Faces and Fingers: Authentication" (2020) 20 J High Tech L 61; Sacharoff, *supra* note 20 at 229; Laurent Sacharoff, "What Am I Really Saying When I Open My Smartphone: A Response to Orin S. Kerr" (2018) 97 Tex L Rev Online 63 at 67; Uresk, *supra* note 1163 at 619.

[1240] See *inter alia Matter of Single-family Home & Attached Garage*, *supra* note 1060; *United States v Kirschner*, *supra* note 1035; *In Re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, *supra* note 1049.

[1241] Cohen & Park, *supra* note 3 at 202. See also Brejt, *supra* note 948 at 1195; Engel, *supra* note 1239 at 561.

[1242] Caren Myers Morrison, "Passwords, Profiles, and the Privilege Against Self-Incrimination: Facebook and the Fifth Amendment" (2012) 65 Ark L Rev 133 at 147.

[1243] *Nedelcu*, *supra* note 393 at para 9.

[1244] Cohen & Park, *supra* note 3 at 209; Hill-Smith, *supra* note 150 at 183.

[1245] Brejt, *supra* note 948 at 1197.

Decryption, then, is a "statement of substance in and of itself,"[1246] whether the password is alphanumeric or biometric.[1247] To state it more simply, decrypting a device produces self-incrimination at different levels, including because decryption implies recognition of "ownership and control of the [devices] and their contents, knowledge of the fact of encryption, and knowledge of the encryption key."[1248]

Recognition of possession and control raises self-incrimination considerations generally, but also more specifically when it comes to offences of possession, such as possession of child pornography (s. 163.1(4) of the *Criminal Code*), possession of a device to obtain unauthorized use of computer system or to commit mischief (s. 342.2 of the *Criminal Code*), or possession of a voyeuristic recording for a prohibited purpose (s. 162(4) of the *Criminal Code*), to name a few. In these specific instances, the act of decryption comes very close to being an admission of guilt in its purest form. The act of decryption can also convey authorship when it comes to evidence, such as text messages or other forms of communications, which can also potentially be relevant to establish the *actus reus* in some cases.[1249] Brejt has even suggested that the principle against self-incrimination could be interpreted as warranting a complete bar on compelled decryption in such cases, except for sentencing purposes.[1250]

[1246] Reitinger, *supra* note 1239 at 70.

[1247] See also Goldman, *supra* note 211 at 221; Metz, *supra* note 936 at 452; Brejt, *supra* note 948 at 1184–1185; Herrera, *supra* note 212 at 800; Redfern, *supra* note 215.

[1248] *Commonwealth v Gelfgatt*, *supra* note 1055 at 615, cited in Cohen & Park, *supra* note 3 at 208.

[1249] Such as uttering threats (s. 264.1 of the *Criminal Code*) or public incitement of hatred (s. 319 of the *Criminal Code*). This was found relevant in *Jones II*, *supra* note 249 at para 23, when Côté J. came to the conclusion that an accused should be allowed to rely on the Crown's evidence to establish the existence of a direct interest in the subject matter of the search, as to not infringe the principle against self-incrimination.

[1250] Brejt, *supra* note 948 at 1186–1187.

A minority of authors have suggested that the act of decryption is only communicative of the ability to decrypt, *sans plus*. Most prominently, Orin S. Kerr has argued that the act of decryption does not imply knowledge of the contents of the device, nor possession or control over the device.[1251] However, users of electronic devices and encryption technologies are unlikely to distinguish the act of decryption from an assertion of possession or control over the device because of the specific usage they make of them. Indeed, most users of devices will keep their own passcodes private or will only set up their own biological features to unlock a device. This is especially true when it comes to cell phones, as most Canadians probably have their own device, one that is not shared with others. Likewise, most users will be aware of the contents of their devices, except perhaps when it comes to the metadata created automatically by the device. Accordingly, the trier of fact, who is most likely also a user of these technologies, will draw strong inferences of possession and control when a suspect is able to unlock a device,[1252] whether with an alphanumeric passcode or with a biometrical authentication measure. In other words, the act of decryption is incriminating by nature.

Multiple lower courts have recognized that compelled decryption does indeed implicate the principle against self-incrimination, in cases involving different types of passwords and locking mechanisms.[1253] First, the Court of Appeal of Quebec in *R c Boudreau-Fontaine* found that forcing the accused to reveal his alphanumeric password with the use of a s. 487

[1251] Kerr, *supra* note 3 at 14. See also Jarone, *supra* note 46 at 795; Nathan D Lyon, "Compelling Decryption of a Smartphone under the Fifth Amendment" (2021) 5:1 Utah J Crim L 57 at 67.
[1252] Sacharoff, *supra* note 1239 at 71.
[1253] Only one court seems to have concluded otherwise, in the specific context of border searches: *R v Buss*, 2014 BCPC 16 at para 33. *Buss* has been criticized as "terse" and unconvincing. See Robert J Currie, "Electronic Devices at the Border: The Next Frontier of Canadian Search and Seizure Law?" (2016) 14:2 CJLT 289.

warrant compelled him to reveal information that would be used to find him guilty of offences related to the use of his device, which triggers the principle against self-incrimination.[1254] In reaching this conclusion, the Court specified that rules emanating from the principle, such as the right to remain silent and the presumption of innocence, were also engaged by such use of s. 487 of the *Criminal Code*.[1255]

Second, in *R v Shergill*, the Ontario Court of Justice concluded that the principle against self-incrimination and its subset right to silence were triggered when it comes to the use of a s. 487.02 assistance order to compel an individual to unlock an electronic device that is password-protected.[1256] The Court also specified that this conclusion remains accurate whether the password has evidentiary value in itself or not.[1257] The same conclusion was also reached in *R v Talbot*, this time in relation with a device protected with a "swipe-pattern."[1258]

Third, in *Impression Warrant Application (Re)*, the Ontario Court of justice reached a similar conclusion, but this time in relation to a biometric authentication method.[1259] In this case, law enforcement sought the issuance of an impression warrant under s. 487.092 of the *Criminal Code* to compel the target to unlock their phone that was password protected but also had a biometric authentication method activated, namely fingerprint recognition. While examining whether this provision of the *Criminal Code* could be used in this manner, the Court

[1254] *R c Boudreau-Fontaine*, *supra* note 779 at para 39.
[1255] *Ibid*.
[1256] *R v Shergill*, *supra* note 230 at para 16.
[1257] *Ibid* at paras 18–19.
[1258] *R v Talbot*, *supra* note 1179. A "swipe pattern" or "pattern lock" is a type of locking mechanism that can replace a password or biometric authentication method. In this case, the device is unlocked when the use "traces a finger over the screen in a specific, personalized pattern." See Mohan & Willasenor, *supra* note 1228 at 25.
[1259] *Impression Warrant Application (Re)*, *supra* note 1180.

concluded in *obiter* that the principle against self-incrimination raised important concerns as to the possibility of compelling an individual to aid the police in this manner.[1260]

It seems clear then that Canadian jurisprudence on self-incrimination does not (and should not) distinguish between alphanumeric passwords, biometric authentication method, or any other type of locking mechanism that can be used to restrict access to a device or to data. The encryption mechanism does not modify the testimonial qualities of decryption, nor its incriminating potential generally. Courts have rather focused on what law enforcement is truly trying to obtain when compelling an individual to decrypt, which is the information that is hidden by encryption. As such, the principle against self-incrimination is applicable at large when it comes to compelled decryption.

In sum, the protection against self-incrimination is indeed applicable when it comes to compelled decryption. Compelling a suspect to unlock a device or to decrypt data removes the *choice* that individuals have to collaborate or engage with the authorities, which is effectively what the overarching principle against self-incrimination seeks to limit.[1261] A parallel can be made here with derivative use immunity, under s. 7 of the *Charter*. As the SCC specified in *Thomson Newspaper*, derivative evidence implicates the principle against self-incrimination by "virtue of the circumstances of [its] discovery in a particular case."[1262] Similarly, compelled decryption implicates the principles against self-incrimination because it will give law enforcement access to evidence that would otherwise be out of their reach absent the compulsion. The question remaining is what exactly the principle requires in this

[1260] *Ibid* at para 15.
[1261] See Chapter 4 *supra*; *Hebert*, *supra* note 384 at 175; Iftene, *supra* note 413 at 27.
[1262] *Thomson Newspaper*, *supra* note X at 550.

context: a complete ban on compelled decryption or the creation of a framework that makes compelled decryption constitutionally possible.

C) Determination of Whether the Deprivation Has Occurred in Accordance with the Relevant Principle of Fundamental Justice

In *White*, the SCC stated that the application of the principle against self-incrimination dictates a flexible approach that considers the context and required "different things at different times."[1263] Particularly when it comes to the determination of whether a provision or power amounts to a violation of the principle against self-incrimination, as a principle of fundamental justice, the SCC used in *White* a series of four factors that were derived from *Fitzpatrick*: (1) the existence of coercion; (2) the presence of an adversarial relationship; (3) the prospect of unreliable confessions; and (4) the potential for abuse of power.[1264]

In *Hart*, one of the most recent SCC decision to consider how the principle against self-incrimination can impose constraints on a specific investigative technique, the majority decided not the follow the *White/Fitzpatrick* framework because of the specific concerns that Mr. Big operations raise.[1265] However, in the context of encryption, the framework provides a structure that encompasses the different considerations that are relevant to determining if compelled decryption infringes the principle against self-incrimination.

Indeed, compelled decryption is similar in multiple ways to the investigative techniques examined in *White* and *Fitzpatrick*. In both cases, the SCC was facing an obligation placed

[1263] *White*, *supra* note 388 at para 45. See also *Brown*, *supra* note 416 at para 95.
[1264] *White*, *supra* note 388 at para 51; *Fitzpatrick*, *supra* note 371 at paras 35–48.
[1265] *Hart*, *supra* note 379 at paras 124–125.

upon a suspect to make a declaration in a specific setting and whether this declaration could then be used at trial against the declarant. Similarly, compelled decryption implies forcing a suspect to unlock or decrypt a device (which carries testimonial qualities) and raises the question of subsequent admissibility of both the evidence obtained and the inferences that can be drawn from the act of decryption. Compelled decryption is very different from a Mr. Big investigation, as it does not involve deceit and trickery by the authorities. Further, Justice Karakatsanis, in her dissent, used the *White/Fitzpatrick* framework, proving that it is still very much relevant to this day.[1266] For these reasons, the *White/Fitzpatrick* framework will be followed here.

i. Existence of Coercion

When compelled to decrypt, individuals are coerced into helping the state to gain access to possibly incriminating evidence that concerns them. Generally speaking, then, they are being compelled into assisting the state in their own prosecution, which is a major concern of the principle against self-incrimination.[1267] As stated by Professors Paciocco and Stuesser. ss. 11(c) and 7 of the *Charter* work together to ensure that the state's compulsory powers are not "used as a substitute for a criminal investigation."[1268] As one of the many possible encryption "workarounds," compelled decryption is essentially a substitute for an investigation, as it shortcuts the need to use another "workaround."

[1266] *Ibid* at paras 191–214.
[1267] *P (MB)*, *supra* note 367 at 577–578.
[1268] David M Paciocco & Lee Stuesser, *The Law of Evidence*, 5th ed (Toronto: Irwin Law, 2010) at 303, referring to *BC Securities*, *supra* note 376.

Unless the target voluntarily provides law enforcement access to decrypted data, which entails a renunciation of a *Charter* right, the existence of coercion is fairly evident in the scenario of compelled decryption, as its name indicates.[1269] Contrary to the situation that prevailed in *Fitzpatrick* when it comes to commercial fishing, compelled decryption does not involve a free choice to participate in a specific activity or to cooperate with the authorities; quite the opposite, in fact.[1270] Indeed, the situation is more akin to *White*, in which the SCC concluded that the choice of driving is not "as free as the choice of whether to enter into an industry."[1271] In this day and age, using digital devices seems almost unavoidable in order to be a functioning member of society. In a correlative manner, encryption is necessary in order for individuals for protect their own privacy and to protect themselves against unwanted intrusions, whether by law enforcement or by criminals.[1272] This is especially true when it comes to delocalized data.[1273] The use of encryption is thus not a 'free choice' that can be interpreted as a renunciation to the principle against self-incrimination.

To be fair, individuals are not being coerced into creating the incriminating data,[1274] only into giving law enforcement access to it. In other words, compelled decryption "is about supplying the evidence."[1275] In a scenario where law enforcement is unable (or not willing) to use another encryption "workaround," law enforcement is left with unreadable information without the compelled assistance of the suspect. While the principle against self-incrimination

[1269] As stated by Lamer J. in *Jones I*, *supra* note 343 at 249, coercion is the absence of free and informed consent.
[1270] *Fitzpatrick*, *supra* note 371 at paras 35–36.
[1271] *White*, *supra* note 388 at para 55.
[1272] David Gray, "A Right to Go Dark" (2019) 72:4 SMU L Rev 621 at 643.
[1273] Engel, *supra* note 1239 at 567.
[1274] Voluntarily prepared documents usually do not trigger the protection against self-incrimination, whether in the Canadian or American contexts. See Folkinshteyn, *supra* note 141 at 385.
[1275] Brejt, *supra* note 948 at 1173.

does not protect against the gathering of real evidence without the participation of the accused,[1276] compelled decryption involves a positive action by the suspect in order to make that information readable and understandable to law enforcement.[1277] This positive act can take multiple forms, such as verbally revealing the password to the authorities, entering the password directly without giving it to the authorities, unlocking a device with a biometric feature, or providing law enforcement with a decrypted copy of the data.[1278] Regardless of the exact act law enforcement is trying to compel, the coercive aspect of compelled decryption remains.

When it comes to search and seizure law, the SCC has stated on multiple occasions that it is necessary to focus on what law enforcement is really after.[1279] The same can be said in the context of self-incrimination.[1280] Unlike when using fingerprinting or collecting DNA for identification purposes, law enforcement is not seeking access to the physical attribute when compelling someone to unlock a device with a biometric authentication method.[1281] Rather, it is trying to gain access to real evidence that is hidden behind encryption. In other words, the state is seeking evidence that is *derivative*, as it comes to be in the possession of the state due to compulsion, which is what the principle against self-incrimination seeks to prevent.[1282] Any

[1276] Dalla Guarda, *supra* note 32 at 133–134.
[1277] A parallel can be made here with the various production orders found within the *Criminal Code* and the fact that they all contain an interdiction to be used against the person or entity under investigation. See ss. 487.014(4), 487.015(5), 487.016(4), 487.017(4), and 487.018(5). The inclusion of this limitation seems to be justified, at least partially, by the overarching protection against self-incrimination. This goes to show that it is the production of evidence that triggers the protection against self-incrimination, not the creation of the evidence itself.
[1278] Cohen & Park, *supra* note 3 at 174.
[1279] See for example *Marakah*, *supra* note 260 at para 16; *Spencer*, *supra* note 241 at para 32; *Cole*, *supra* note 30 at para 41.
[1280] *R v Shergill*, *supra* note 230 at para 19, referring to *Reeves*, *supra* note 250 at paras 30–31.
[1281] Metz, *supra* note 936 at 452, 455; Brejt, *supra* note 948 at 1170; Herrera, *supra* note 212 at 801.
[1282] *S (RJ)*, *supra* note 343; Robert Diab & Marshall Putnam, "Is Password Compulsion Constitutional in Canada? Two Views" (2019) 77:4 Advocate 513 at 516.

analysis that equates compelled decryption using biometric authentication methods to identification procedure using physical characteristics[1283] misses the point, as compelled decryption is fundamentally different from compelled identification.[1284] Accordingly, current provisions regarding fingerprinting should not be used to compel individuals to unlock their devices uses a biometric authentication method, as decided in *Impression Warrant Application (Re)*.[1285]

It could be argued that decryption of devices using facial recognition as unlocking mechanism does not involve coercion, as the device can simply be raised in front of the owner of the device to unlock it. This may indeed be true when we focus on the passivity that this entails on the suspect's end. However, the choice to use a specific locking mechanism should not be used to afford less rights to individuals when this mechanism is functionally equivalent to any other type of encryption key. Locking mechanisms that use facial recognition involve the same objective as fingerprint locks or alphanumeric passcodes: keeping intruders out of personal data. Conceived in this manner, placing a device in front of the subject's face can be perceived as being coercive, as it forces that individual to unlock the device while they do not

[1283] See for example Cole, *supra* note 213 at 188; Lyon, *supra* note 1251 at 62; Erin M Sales, "The Biometric Revolution: An Erosion of the Fifth Amendment Privilege to Be Free from Self-Incrimination" (2014) 69 Univ Miami L Rev 193; Shweiki & Lee, *supra* note 1002 at 37.

[1284] As put by the U.S. District Court of Northern Illinois in *In Re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, *supra* note 1049, cited in Czerniawski & Boyack, *supra* note 298 at 80:

> "We do not believe that a simple analogy that equates the limited protection afforded a fingerprint used for identification purposes to force fingerprinting to unlock an Apple electronic device that potentially contains some of the most intimate details of an individual's life (and potentially provides direct access to contraband) is supported by Fifth Amendment jurisprudence."

See also *US v Sealed Warrant*, 2019 WL 4047615 and *In re Search of Residence in Oakland, C.A.*, *supra* note 1060, both cited in Lea M Solakian, "The Key to Compelled Decryption: Beyond a Reasonable Doubt" (2021) 27:2 Widener L Rev 219 at 232.

[1285] Gill, Israel & Parsons, *supra* note 3 at 70.

want to do so. The coercion felt by the individual is the same regardless of the encryption method.[1286]

Simply put, any method to gain access to a device or to data using the assistance of the suspect will be coercive in nature because the suspect is being forced into helping the state to reach evidence that could not have been obtained otherwise. For this reason, it has been suggested that the principle against self-incrimination should be interpreting as barring compelled decryption altogether.[1287] However, not all compulsion by the state towards its citizens is contrary to the principle against self-incrimination.[1288] One has to think only of compelled production of DNA for investigative purposes or compelled sobriety testing to realize that the state can compel some degree of self-incrimination in various situations.[1289] However, compelling incriminating statements from a suspect is barred altogether by the right to remain silent.[1290] In other cases, the context is important to delimitate the contours of the protection against self-incrimination.

When it comes to compelled decryption, the distinction lies in the fact that the incriminating aspect of decryption lies mostly within the act of decryption, as opposed to the material in itself (which is however protected by s. 8 of the *Charter*). As with compelled sobriety testing, the *testimonial* self-incriminating act gives access to *non-testimonial* evidence. As put by Penney and Gibbs:

[1286] This has implicitly been accepted by the many US courts that have deemed biometric authentication measures to be the equivalent of alphanumeric passcodes. See Section 6.3.1(B) *supra*.
[1287] Gill, Israel & Parsons, *supra* note 3 at 69.
[1288] *Fitzpatrick*, *supra* note 371 at paras 21–24, 29–32.
[1289] See Chapter 4 *supra*.
[1290] See Section 7.3.1(A) *infra* on the possible impact of *Mills II* on this statement.

> 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.[1291]

This is why act of decryption immunity can properly address the self-incriminating aspect of compelled decryption (i.e., the testimonial aspect of decryption). Contrary to "traditional" self-incriminating statements, the state is not after the statement in itself, but rather what the statement gives access to. This also forces the conclusion that without act of decryption immunity, compelled decryption would contravene the right to remain silent, as it is a compelled self-incriminating statement. The safeguards put in place to prevent the use of that statement to establish guilt is what makes compelled decryption possible.[1292]

ii. Presence of an Adversarial Relationship Between the Suspect and the State

At the time the sought-after data was created, the individual was not in an adversarial relationship with the state.[1293] When under investigation for a possible criminal law offence, however, individuals are quite obviously in an adversarial relationship with the state, one that cannot be qualified as being a partnership.[1294] This remains true even if the adversarial

[1291] Penney & Gibbs, *supra* note 3 at 234, referring to the SCC's decision in *Orbanski*, *supra* note 442.
[1292] This is coherent with the SCC's decision in *SAB*, where it was decided that compelled production of DNA evidence, while self-incriminating, was nonetheless permissible because of the stringent conditions put in place by the DNA warrant provisions. See *SAB*, *supra* note 430 at para 59. It is also tempting to draw a parallel here with *Nedelcu*, where the majority focused heavily on the *incriminating* nature of the evidence. Here, by removing the *incriminating* nature of compelled decryption, s. 7 considerations are neutralized.
[1293] *Ibid* at 236.
[1294] *White*, *supra* note 388 at para 58; *Fitzpatrick*, *supra* note 371 at para 36.

relationship between the state and the compelled individual has not yet concretized itself at the time of compulsion.[1295] Accordingly:

> any government sanctioned act of compelling decryption must be seen within the context of an adversarial relationship between the accused and the state where, furthermore, the "predominant purpose" of the testimony if to incriminate the accused through the evidence thereafter acquired.[1296]

The imbalance between the state and the individual that comes from this adversarial relationship is what justifies the principle against self-incrimination.[1297] In other words:

> Our constitutional law protects the right against self-incrimination because we recognize there is a power imbalance in criminal prosecutions, which frequently pit a single (often marginalized) individual against the overwhelming power of the state. The right against self-incrimination is the great equalizer. It ensures an individual is put through the criminal process only once police have built a case. It also protects the dignity of the accused and limits the risk that state officials will abuse their power. [1298]

iii. Presence of an Increased Risk of Unreliable Confession as a Result of the Statutory Compulsion

The principle against self-incrimination has been given two modern underlying rationales: (1) protection against unreliable confessions; and (2) protection against the abuse of power by the state.[1299] Real evidence is considered highly reliable because of its material existence,

---

[1295] *Brown*, *supra* note 416 at para 94.
[1296] Dalla Guarda, *supra* note 32 at 134.
[1297] *P (MB)*, *supra* note 367 at 577–578; *Dubois*, *supra* note 360.
[1298] Nader R Hasan & Stephen Aylward, "Password protection a crucial Charter right", (23 August 2016), online: *The Star* <https://www.thestar.com/opinion/commentary/2016/08/23/password-protection-a-crucial-charter-right.html>.
[1299] *Jones I*, *supra* note 343 at 250.

which militates against a recognition that the principle against self-incrimination completely bars such coercive investigative techniques, as compelled decryption essentially gives the state access to real evidence. However, this does not mean that compelled decryption does not raise a risk of unreliable confession in different, more limited, sense.

If we focus on the act of decryption as conveying a statement of ownership or control over the device or data, we could see situations where the act of decryption is indeed unreliable. For example, an individual may unlock a device that belongs to someone else, which could then be used against them in at trial under the pretense that they had control and possession over the device and its contents. This inference of control or possession is, in this scenario, false and places a burden on the accused to prove that the device did not actually belong to them, which raises important self-incrimination considerations, mostly under the presumption of innocence.

Further, the compulsion to decrypt can also place the suspect in a situation where an incentive to lie or otherwise falsify information is present. To use the American "cruel trilemma" analysis,[1300] individuals facing compelled decryption have the choice to: (1) tell the truth by decrypting the device or data, giving law enforcement access to the possible incriminating evidence and the strong inferences that they have possession and control over it; (2) falsely pretend that they cannot decrypt the data, which could mean facing obstruction or contempt if the prosecution can prove that it was done wilfully and that the individual had the means to decrypt; or (3) refuse to decrypt, with the same potential for prosecution.[1301]

[1300] See Section 6.1.1 *supra*.

[1301] Bales, *supra* note 943 at 1304. See also Bonin, *supra* note 6 at 513; Brejt, *supra* note 948 at 1160; Sacharoff, *supra* note 20 at 227.

Penney and Gibbs conclude that compelled decryption raises no issues when it comes to the risk of unreliable confessions, mainly because it will be immediately apparent if the individual is not telling the truth by not providing the proper decryption key.[1302] However, this conclusion does not account for the reality that individuals tend to forget their passwords, especially ones used to access websites (as opposed to passwords used more regularly to unlock a device for example). A declaration of guilt to an obstruction or contempt charge thus is very possible, even if the individual had every intention of respecting the order to decrypt.[1303] In other words, an individual compelled to unlock a device might be unable to decrypt it, falsely leading the court to think that they refused to do so.

It has been suggested that decryption carries no testimonial quality—and thus raises no self-incrimination considerations—if the state is already able to prove ownership and control over the device independently from the act of decryption.[1304] This has been suggested in the American context, where the "foregone conclusion doctrine" has been determined to remove the testimonial aspects of producing evidence. This doctrine does not find an equivalent in Canadian criminal law but can be used as a jumping-off point to mitigate the consequences that stem from the act of decryption.[1305]

[1302] Penney & Gibbs, *supra* note 3 at 237.
[1303] As put by Brejt, *supra* note 948 at 1181: "it would be a miscarriage of justice if individuals were held in contempt for genuinely not knowing a password."
[1304] Colarusso, *supra* note 6 at 86.
[1305] See Section 7.3.2 *infra*.

Additionally, if the punishment for the main crime under investigation is more severe than for a potential prosecution for failure to respect a decryption order, the incentive to refuse to decrypt is very present.[1306]

iv. Presence of an Increased Risk of Abuses of Power by the State as a Result of the Statutory Compulsion

In establishing its jurisprudence on the principle against self-incrimination, the SCC was cognizant of the risk that coercing individuals into self-incriminating is a "slippery slope towards the creation of a police state."[1307] The determination that the principle against self-incrimination is not triggered by compelled decryption would create potential for the abuse of state power, especially when examined in relation with the jurisprudence on the search and seizure of digital devices and evidence.

In recent years, the SCC has granted far-reaching search and seizure powers to law enforcement when it comes to digital devices: *Fearon* gave law enforcement the power to conduct warrantless searches of cell phones incident to arrest,[1308] while *Vu* stated that *ex ante* conditions should not generally be imposed when it comes to regulating the search of computers.[1309] Combined with the fact that court authorizations are easily obtained by law enforcement[1310] and that multiple courts have concluded that a search of the entire device will often be required in order to find all relevant evidence,[1311] these conclusions raise important

[1306] Brejt, *supra* note 948 at 1181.
[1307] *Thomson Newspapers Ltd v Canada*, *supra* note 345 at 480, also cited in *Jones I*, *supra* note 343 at 250–251.
[1308] *Fearon*, *supra* note 1.
[1309] *Vu*, *supra* note 1 at paras 53–59.
[1310] Sacharoff, *supra* note 20 at 214. See also Cruess, *supra* note 860.
[1311] See *inter alia Uber Canada inc c Agence du revenu du Québec*, *supra* note 777 at paras 281–284.

privacy and self-incrimination questions.[1312] If law enforcement was able to compel suspects to unlock their devices without judicial oversight, the potential for abuse would be very high considering the unique nature of personal devices and the nature and amount of data they contain.[1313]

Distinguishing between locking mechanisms would be especially worrisome when combined with the doctrine of search incident to arrest, as cellular devices are now increasingly protected with biometric authentication methods.[1314] The prospect that the principle against self-incrimination does not apply to devices using this type of encryption mechanism effectively would remove the last protection against law enforcement abusing this warrantless search power.

By reuniting ss. 7 and 8 of the *Charter*, it is also possible to see the risk of 'fishing expeditions,' a specific type of potential abuse of power, being amplified by compelled decryption.[1315] Law enforcement agents will sometimes be given access to devices without having reasons to search them, for example when collecting a person's possessions after an arrest, in a situation where they do not need to search the device incident to arrest. These cases create a very real potential for 'fishing expeditions' if law enforcement is given the power to

---

[1312] Adriana Christianson, "Locked out or Locked up: The Need for New Guidelines for Compelled Decryption" (2022) 55:2 Suffolk U L Rev 237 at 232.

[1313] Jenna Phelps, "It is Only a Fingerprint: Biometric Compulsion and the Fifth Amendment" (2020) 89:2 UMKC L Rev 461 at 473; *Morelli*, *supra* note 30 at paras 2–3; *Vu*, *supra* note 1 at para 2; *Fearon*, *supra* note 1 at para 51.

[1314] It is estimated that 66% of smartphone owners will use biometric authentication methods by 2024. See Payments Journal, "By 2024, How Many Smartphone Owners Will Use Biometrics?", (4 June 2020), online: *PaymentsJournal* <https://www.paymentsjournal.com/by-2024-how-many-smartphone-owners-will-use-biometrics/>. See also Herrera, *supra* note 212 at 805.

[1315] As stated by Penney & Gibbs, *supra* note 3, the risk of "fishing expeditions" is usually considered under a s. 8 analysis. Here, by reconciling both provisions, it is submitted that this risk is also relevant under self-incrimination considerations. See also Sacharoff, *supra* note 20 at 247–248.

compel decryption without a valid court order. This is especially true when law enforcement is seeking access to devices found in a shared home and if law enforcement compels every resident to try to decrypt the devices.

This increased risk of abuse can be mitigated by making compelled decryption only available to law enforcement under a strict prior authorization scheme.[1316] This court authorization would only be available when no other encryption "workaround" is available to law enforcement once they legally obtain the device or data, reflecting the heightened privacy and self-incrimination interests individuals have towards their devices, their data, and the method they choose to protect these. The imposition of strict requirements was found to sufficiently alleviate the self-incrimination impacts of DNA search warrants in *SAB*, in order to safeguard these provisions under s. 7 of the *Charter*.[1317] It is contented here that the same principles apply when it comes to compelled decryption.

The prospect of having to obtain prior judicial authorization before being able to compel a suspect to decrypt may raise certain objections from law enforcement. Primarily, the issue of timing may be raised, as well as the potential that evidence will be remotely deleted. However, law enforcement is not entitled to the most efficient or effective investigative techniques.[1318] Rather, law enforcement is allowed to use techniques that reasonably interact with citizens' rights. Further, some technologies can mitigate the risks that law enforcement face, such as

[1316] See Section 7.3.1 *infra*.
[1317] *SAB*, *supra* note 430 at para 59.
[1318] As put by Czerniawski & Boyack, *supra* note 298 at 83, "[w]hile it is true that a person's securing of their device may make law enforcement's job harder if they are unable to gain access to the device, criminal investigation and prosecution was never meant to be easy."

the use of "Faraday bags."[1319] The power to compel decryption should not be merely convenient for law enforcement, it should be limited to cases where it is absolutely necessary, due to the unique and strong interests at play.[1320]

7.2.2 Section 8 Considerations Towards the Encrypted Material

In addition to the recognition that compelled decryption triggers the principle against self-incrimination because of the testimonial quality of the act of decryption, it is also possible to conceive it as raising self-incrimination considerations because it will effectively give the state access to real evidence that will be used to "prove guilt."[1321] In other words, the act of decryption "furnish[es] a link in the chain of evidence" that is necessary to prosecute the suspect.[1322] Conceiving self-incrimination in this manner can be challenging because the gathering of real evidence by the state is usually considered solely under the privacy protection granted by s. 8 of the *Charter*. However, the positive act required by the suspect in order for the state to gain access to the real evidence (i.e., the act of decryption itself) fundamentally shifts the discussion from "traditional" search and seizure law to a place where self-incrimination and search and seizure law must coexist.

As mentioned, the SCC has already considered self-incrimination considerations under s. 8 of the *Charter* in *R v SAB*.[1323] As such, the self-incrimination and privacy aspects related to

[1319] *R v Jones*, 2019 ONCJ 805 at para 71. A "faraday bag" is an aluminum bag that prevents any radio communication from or to the phone, which prevents transmission of data and remote deletion of data. See Nader R Hasan, "A Step Forward of Just a Sidestep? Year Five of the Supreme Court of Canada in the Digital Age" (2015) 71 SCLR (2d) 439–474 at 440 at 458; *Fearon*, *supra* note 1 at para 144.
[1320] This directly answers Robert Diab's question. Diab, *supra* note 3 at 284.
[1321] *Nedelcu*, *supra* note 393 at para 9; *Kuldip*, *supra* note 357 at 633; *Henry*, *supra* note 354 at para 25.
[1322] Engel, *supra* note 1239 at 545, citing *Hoffman v United States*, 341 US 479 (1951); *Blau v United States*, 340 US 159 (1950). See also Leamon, *supra* note 1239 at 603; Mahoney, *supra* note 46 at 92.
[1323] *SAB*, *supra* note 430 at para 35.

the encrypted material itself are better suited to an analysis under s. 8 of the *Charter*, starting with the application of the reasonable expectation of privacy test.[1324]

A) Application of the Reasonable Expectation of Privacy Test to Compelled Decryption

As dictated by the SCC in many cases, the existence of a reasonable expectation of privacy dictates whether a specific investigative technique can be qualified as a search or a seizure, triggering the application of s. 8 of the *Charter*. The *Tessling* "totality of circumstances test" will be utilized to determine if this in the case with compelled decryption.[1325]

i. Identification of the Subject Matter of the Alleged Search

When compelling a suspect to decrypt, law enforcement is not seeking access to the physical device itself.[1326] Rather, if we focus on what the state is actually trying to obtain,[1327] the subject matter of a compelled decryption order is above all the data that is hidden behind encryption. Further, because the act of decryption communicates the ability to decrypt, it is also possible to conceive the subject matter of the search as implicating the assertion of ownership or control over a device or over data.[1328]

[1324] Maybe it is worth restating here that the principle against self-incrimination itself is partly justified by a desire to promote and protect individual privacy. As such, the decision to analyze some self-incrimination considerations under s. 8 is logical. See *Thomson Newspapers Ltd v Canada*, *supra* note 345 at 480.
[1325] *Tessling*, *supra* note 250 at para 32. See also *Edwards*, *supra* note 235 at para 45; *Patrick*, *supra* note 571 at para 27; *Cole*, *supra* note 30 at para 40; *Spencer*, *supra* note 241 at para 18; *Marakah*, *supra* note 260; *Jones II*, *supra* note 249; *Reeves*, *supra* note 250; *Mills II*, *supra* note 264 at para 13.
[1326] See *inter alia Cole*, *supra* note 30 at para 41.
[1327] *Marakah*, *supra* note 260 at para 15.
[1328] Penney & Gibbs, *supra* note 3 at 242.

On a lesser level, the decryption key or biometric marker itself is also sought-after, but only in respect of its unlocking function. As put by Herrera:

> when using a fingerprint to unlock a smartphone, the fingerprint is not helping the government identify the source of an unknown fingerprint. Rather, it is serving the functional equivalence of a password by allowing access to a phone, thereby giving access to a flood of personal information about the smartphone's owner.[1329]

As such, any decryption mechanism is sought after for its unlocking purpose. Essentially, the locking mechanism serves as a proxy for the privacy interests in the data itself. Encryption's goal is to protect personal data from being accessible and readable to third parties.[1330] Distinguishing encryption from the data itself is rather illusory;[1331] so is distinguishing between the act of decryption and the data itself.[1332] Individuals activate encryption measures specifically to protect data that concerns them, whether on their devices directly, in the cloud, or when using communication platforms. Accordingly, the subject matter of a decryption order should be conceived broadly and defined as encompassing the data itself, the encryption key in whatever form it takes, and the inferences it allows the state to draw.

[1329] Herrera, *supra* note 212 at 801.

[1330] Candice Gliksberg, "Decrypting the Fourth Amendment: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Encryption Technology" (2017) 50:4 Loy LA L Rev 765 at 773.

[1331] As put by Flynn, *supra* note 1190 at 12, "[t]he average person is unlikely to understand that unlocking a phone and providing consent to search the phone are two different actions, with different legal consequences." As such, jurists should be cautious of conceiving the act of decryption has being so distant from the data itself that it does not warrant an examination under ss. 7 and 8 of the Charter.

[1332] Rangaviz, *supra* note 1176 at 184.

ii. Existence of a Direct Interest in the Subject Matter

As previously stated, the act of decryption is a strong indicator of ownership or control over a device. The ability to decrypt then, real or alleged by the prosecution,[1333] is sufficient to establish a direct interest in the subject matter of the search. Further, the fact that encrypted personal data or the passcode itself is sometimes shared with TPDCs does not remove a direct interest in the subject matter of the search.[1334] As such, the fact that the encrypted data is stored on a remote cloud for example, does not require us to forego the analysis under s. 8.

Individuals also have a direct interest in their biometric features that can be used to decrypt. Accordingly, it could be argued that bodily privacy is also triggered by compelled decryption, in cases where the device is protected by a biometric authentication measure.[1335] However, the impact of compelled biometric decryption on bodily privacy and autonomy is very minimal when considering the physical gesture required to unlock a device with either a fingerprint or one's face. Further, when focusing on what the biometrical feature grants access to, the fact that the "key" in this case exists physically does not change the fact that it is used to access data, making it predominantly about informational privacy.

iii. Existence of a Subjective Expectation of Privacy

The act of password-protecting a device is an assertion of personal privacy towards the device and its contents.[1336] Whether we define privacy as being about our control over information

[1333] *Jones II*, *supra* note 249 at para 29.
[1334] See Section 5.2.2 *supra*.
[1335] See for example Redfern, *supra* note 215 at 627.
[1336] Lemus, *supra* note 220 at 556. See also Abe Andrew Bailey, "Privacy, Privilege, and Protection: A Case for Fifth Amendment Expansion" (2019) 29:2 U Fla JL & Pub Pol'y 167 at 187; Lowell, *supra* note 221 at 502.

that concerns us,[1337] access to this information,[1338] or more generally about a "right to be let alone,"[1339] encryption is the ultimate embodiment of privacy.[1340] In other words:

> This sense of complete privacy when encrypting a document should be seen as an affirmative step aimed at creating a reasonable expectation of privacy. Those that actually encrypt their documents are taking affirmative steps above and beyond the steps taken by regular computer users. Those that encrypt are attempting to ensure that their documents will remain secure by building an electronic safe around their electronic property. As a consequence, it can be argued that someone that encrypts is exhibiting an actual expectation of privacy in relation to specific documents that he or she encrypts.[1341]

More than that, users of encryption also have a subjective expectation of privacy towards the encryption key itself, in whatever form it may take. Users are instructed not to divulge their passcodes and encryption keys[1342] and not to note them down on a piece of paper or a notebook.[1343] Further, users definitely have a subjective expectation of privacy towards their data itself; this much is clear from the SCC's jurisprudence on digital privacy.[1344]

[1337] Westin, *supra* note 239 at 7.
[1338] Molitorisz, *supra* note 232 at 133.
[1339] Warren & Brandeis, *supra* note 236. See also Section 3.1 *supra*.
[1340] Lemus, *supra* note 220 at 559.
[1341] Sean J Edgett, "Double-Clicking on Fourth Amendment Protection: Encryption Creates a Reasonable Expectation of Privacy" (2003) 30:2 Pepp L Rev 339 at 350. See also West & Forcese, *supra* note 85 at 10, on the idea that the use of encryption to hide one's identity is also indicative of an enhanced expectation of privacy.
[1342] For example, Dalhousie's acceptable use policy concerning email and passwords specifies that "disclosing passwords or other access codes assigned to themselves or others" is an unacceptable activity because it is not secure. See Dalhousie, "Acceptable Use Policy", (February 2020), online: *Dalhousie University* <https://cdn.dal.ca/content/dam/dalhousie/pdf/dept/university_secretariat/policy-repository/Acceptable%20Use%20Policy%20Feb%202020.pdf>.
[1343] See for example IBM, "Password guidelines", (7 April 2022), online: *IBM* <https://www.ibm.com/docs/en/aix/7.2?topic=passwords-password-guidelines>.
[1344] See *inter alia Cole*, *supra* note 30 at para 43, in which the SCC mentions that the use an individual makes of a device allows for strong inferences of a subjective expectation of privacy.

When using a biometric feature to lock and unlock their devices, users expect the feature to serve the same purpose as an alphanumeric passcode, making it the subject of the same subjective expectation of privacy. It could possibly be stated that individuals do not expect their facial feature to remain private, due to the fact that they are exposed to the public continuously.[1345] However, when combined with the purpose of the biometric lock, it is clear that users maintain a subjective expectation that their facial features will not be used to unlock a device without their consent.[1346] If anything, it is more likely that the use of biometric locks indicates a heightened subjective expectation of privacy, considering that biometric features are not replicable.

iv. Objective Reasonableness of an Expectation of Privacy

In recent years the SCC has tried to adapt its jurisprudence on privacy to fit the new paradigm brought forward by communications technologies. This, as stated previously, has not always been entirely coherent. The SCC's jurisprudence on privacy in the digital age shows that the choice between "technological neutrality" and "technological novelty" has involved fluctuations which make the determination of the objective reasonableness of an expectation of privacy difficult to predict. This is also due to the fact that 'traditional' factors used to determine the presence of a reasonable expectation of privacy, namely the *Edwards* factors,[1347] are ill-suited to this analysis, mostly because they were developed in the analog world.

[1345] *Tessling*, *supra* note 250 at para 47; *R v Boersma*, [1994] 2 SCR 488.

[1346] To some degree, the fact that facial recognition only functions when the user has their eyes open indicates this. See Apple, "About Face ID Advanced Technology, (27 April 2022), online: *Apple Support* <https://support.apple.com/en-us/HT208108>.

[1347] *Edwards*, *supra* note 235 at para 45.

On one side, the adoption of the "technological novelty" approach in decisions such as *Vu*, *Spencer*, and *Marakah*, or in dissent by Martin J. in *Mills*, hints at the possibility that the subject matter of a decryption order (properly identified as being the data found in the device, the encryption key, and the inferences that stem from the act of decryption) would be found to be protected by an objectively reasonable expectation of privacy. It is objectively reasonable for individuals to expect that the state would not be allowed to force them to unlock their devices (or decrypt their data) at its sole discretion. As encryption is seen as one of the last ramparts of digital privacy, individuals are entitled to expect that the state would not undermine the purpose of encryption (i.e., preventing unwanted third parties from accessing the protected data) by being allowed to compel decryption without prior judicial authorization.

Following recent events that encouraged the rise of encryption technologies, such as the Snowden revelations, users of digital technology have resorted to encryption to protect their digital privacy.[1348] Encryption serves as "a precaution that increases electronic communications privacy."[1349] Indeed, without encryption, digital privacy is non-existent, especially when it comes to 'data in transit.' The unique nature of personal digital devices, particularly cell phones, also warrants strong privacy protections for 'data at rest,' due to the quantity of information that can be found on them. Encryption keys, passcodes, and biometric authentication methods are an effective method to protect privacy and should attract a reasonable expectation of privacy as such.

[1348] See *inter alia* Michael Geist, ed, *Law, privacy and surveillance in Canada in the post-Snowden era*, Law, technology and media (Ottawa, Ontario: University of Ottawa Press, 2015); Gray, *supra* note 1272; Amitai Etzioni, "A Cyber Age Privacy Doctrine: More Coherent, Less Subjective, and Operational" (2015) 80:4 Brook L Rev 1263 at 1271.

[1349] Lee Tien, "Doors, Envelopes, and Encryption: The Uncertain Role of Precautions in Fourth Amendment" (2005) 54:3 DePaul L Rev 873.

The SCC in *Duarte* and *Wong*[1350] was cognizant of the risk that if the state was left unchecked and allowed to make permanent recordings of private communications without prior judicial authorization, privacy would no longer have any meaning.[1351] While compelled decryption is not electronic surveillance *per se*, the same conclusions can be applied to this specific investigative technique. Compelled decryption holds the potential of the state invading our most intimate thoughts and imminently personal information by accessing the data our personal electronic devices hold, in situations where we are forced to help the state to reach its investigative goal and ultimately prosecute us. Allowing the state to do this without obtaining prior judicial authorization brings us uncomfortably close to George Orwell's *1984* novel, which was exactly what the SCC was trying to avoid in *Wong*.[1352] Essentially, compelled decryption by the state—by removing the last protection individuals have to ensure their digital privacy—would imply that we have no privacy interest against the state invading our data, which is untenable in light of *Morelli*, *Cole*, *Vu*, and *Marakah*,[1353] and in light of a normative understanding of privacy.

Encryption is necessary and essential to many activities that can be conducted online, from e-commerce, to communications, and everything in between.[1354] It protects consumers against

---

[1350] Two decisions that can be categorized under the "technological novelty" approach.
[1351] *Duarte*, *supra* note 607 at 44; *Wong*, *supra* note 567 at 47.
[1352] *Wong*, *supra* note 567 at 47.
[1353] *Fearon* was not included here because it is an outlier in the SCC's jurisprudence on the degree of privacy individuals can expect to have over their electronic devices. It also falls under the "technological neutrality" approach that will be discuss *infra*. However, it can be noted that, even in this decision, the SCC recognized that the search of electronic devices implicate important privacy interests. See *Fearon*, *supra* note 1 at para 51.
[1354] Christopher Babiarz, "Encryption Friction" (2017) 10 Alb Gov't L Rev 351 at 355. Essentially, any activity that requires sensitive information to be communicated on a network will use a type of encryption. For example, most websites where sensitive information is communicated now use HTTPS, which is an encrypted and thus secure version of the primary protocol used to communicate data between a device and a website. See Cloudflare, "What is HTTPS?", online: *Cloudflare* <https://www.cloudflare.com/learning/ssl/what-is-https/>. See also Chapter 2, supra.

fraud and identity theft, while also ensuring that companies and governments are secure against hackers.[1355] Even individuals who do not own personal digital devices are impacted by encryption because they will almost invariably conduct business with some entity that collected and encrypted data that concerns them at some point. Normatively then, individuals are entitled to expect that the state cannot weaken or circumvent encryption at will, as it would not only expose them to risk but also undermine the purpose of encryption itself.[1356]

As put by Hamish Stewart, "the ultimate normative question is whether, in light of the impact of an investigative technique on privacy interests, it is right that the state should be able to use that technique without any legal authorization or judicial supervision."[1357] If left unchecked, the state will be able to compel the unlocking of devices and decryption of data whenever it sees fit, without possible supervision from the courts. This would not reflect the importance of encryption as it relates to privacy and self-incrimination and would effectively annihilate the right to keep information private from anyone, including the state.

Because encryption serves as a safeguard for various rights and freedoms,[1358] Parliament and courts should be eager to recognize that the encryption of personal devices is an assertion of an objectively reasonable expectation of privacy, alongside being an assertion of the other *Charter* interests at play, namely self-incrimination. As everyone has a right to privacy and

[1355] Jaffer & Rosenthal, *supra* note 101 at 294.
[1356] This will be especially important when it comes to the possibility of forcing TPDCs to insert backdoors into their systems. See Chapter 8 *infra*.
[1357] Hamish Stewart, "Normative Foundations for Reasonable Expectations of Privacy" (2011) 54 SCLR (2d) 335 at 342.
[1358] Parsons, *supra* note 56. See Section 2.2 *supra*.

benefits from the protection against self-incrimination, everyone also has a right to encryption and to be protected against warrantless compelled decryption.

On the other side, the "technological neutrality" approach would most likely dismiss the claim that the subject matter of a decryption order raises different privacy considerations than the ones linked to the data law enforcement is trying to obtain. This would be consistent with the majority's decisions in *Fearon* or *Mills*, and with Karakatsanis J.'s dissenting reasons in *Mills*, all adopting the "technological neutrality" approach to restore or maintain the traditional investigative powers law enforcement have been benefiting from. Following this approach, as law enforcement has traditionally been able to access data without being encumbered by strong encryption, the impact of this technology on investigations should be alleviated by granting law enforcement powers that restore the traditional balance that existed prior to the advent and proliferation of encryption.

At a minimum, this is true: by recognizing that decryption is mostly about access to the plaintext hidden by encryption, the recognition of a reasonable expectation of privacy should be evident, when considered in light of the SCC's jurisprudence on digital privacy.[1359] As the SCC was quick to recognize a reasonable expectation of privacy towards personal data regardless of protection measures put in place by users, it would surely recognize that encryption makes the existence of a reasonable expectation of privacy towards the protected data even more obvious.

[1359] As put by Agathon Fric, "the idea that an individual has a reasonable expectation of privacy in the contents of his cell phone and other digital devices is no longer the subject of serious legal debate." See Agathon Fric, "Reasonableness as Proportionality: Towards a Better Constructive Interpretation of the Law on Searching Computers in Canada" (2016) 21 Appeal 59 at 64.

However, by defining the subject matter of compelled decryption order in a manner that properly describes what law enforcement is trying to obtain, this is unsatisfactory as it would make compelled decryption available in situations where a judicial authorization has not been obtained by law enforcement, following the SCC's decision in *Fearon*. It would also imply that the existing judicial authorization found in the *Criminal Code* (most likely a s. 487.01 general warrant) can be used to compel a suspect to decrypt a device, which does not reflect the heightened privacy interests at play and the self-incrimination considerations identified previously.[1360]

Taken to the extreme, "technological neutrality" applied to compel decryption could completely negate the application of s. 8 to this investigative technique. As mentioned in Chapter 5, in her dissent in *Reeves* Côté J. concluded that the warrantless seizure of a computer could be distinguished from the search of its contents.[1361] Following this reasoning, the act of decryption could be completely isolated from the privacy interests relating to the device itself and the data it contains, making it only a s. 7 issue. This is unsatisfactory because it would imply that encryption is unrelated to privacy, which is simply untenable in light of the purpose of encryption and the fact that it is inextricably linked to the data it is protecting.

By focusing on how individuals use encryption and its positive applications, it becomes clear that encryption raises additional privacy and self-incrimination considerations when compared to 'traditional' search and seizure of digital evidence. By going back to ss. 7 and 8's shared values, it becomes more obvious that measures put in place by individuals to protect and assert their rights to privacy and against self-incrimination should attract *Charter*

[1360] See Section 7.2.2(A)(v) immediately *infra*.
[1361] *Reeves*, *supra* note 250 at para 123.

protection.[1362] The fact that the SCC has used a normative approach to privacy, as opposed to a descriptive approach, also supports the proposition that encryption attracts a reasonable expectation of privacy.[1363]

A principled approach to privacy and a technologically novel vision of ss. 7 and 8 dictate that a subjective expectation of privacy in the subject matter of a compelled decryption order should be recognized as objectively reasonable.

v. Strength of the Privacy Interest at Play

Having concluded that it is objectively reasonable for someone to expect that the state will not be able to acquire the contents of their devices without prior judicial authorization and that the application of encryption engages a reasonable expectation of privacy, it is necessary to examine whether the strength of that privacy interest is modified when compared to data that is not protected by encryption. Decisions such as *Morelli*, *Cole*, *Vu*, *Marakah*, and *Fearon* make it clear that Canadians' expectation of privacy towards personal data found on their various devices is a reasonable one. What is not as clear from these decisions is whether encryption modifies—either by amplifying or decreasing—a reasonable expectation of privacy towards digital information. The majority of the SCC in *Fearon* mentioned *in obiter* that the absence of a password on a device is not necessarily indicative of a lack of a reasonable expectation of privacy towards the contents of the device but did not examine

[1362] As put by Lemus, *supra* note 220 at 538:

> "[w]hen new developments-whether technological, social, or political in nature-significantly challenge the perceptions and notions Americans have of their basic Constitutional rights, it becomes imperative to take a principled look at these constitutionally-protected guarantees to ensure that these new developments are adapted to conform to the Constitutional framework, rather than vice-versa."

[1363] Dolhai, *supra* note 250 at 5.

whether the password itself was protected by s. 8 of the *Charter*, nor whether encryption could be seen as transforming the strength of the privacy interests at play.[1364] Further, the unique involvement of self-incrimination when it comes to compelled decryption was not been argued in front of the SCC, making this uncharted territory for Canada's highest court.

It is possible to draw a parallel between compelled decryption orders and the obtention of subscriber information by law enforcement. In *Spencer*, the SCC specified that when adequately defining the subject matter of the search as being the identity of an internet subscriber which corresponds to a specific internet usage, it becomes clear that individuals can reasonably expect their subscriber information to be private and not to be disclosed by the ISP to the authorities without a valid court order.[1365] As stated by the Court, "[t]his sort of request engages the anonymity aspect of the informational privacy interest by attempting to link the suspect with anonymously undertaken online activities, activities which have been recognized by the Court in other circumstances as engaging *significant* privacy interests."[1366]

Similarly, if defining the subject matter of a compelled decryption order as being first and foremost the data in the device, it becomes clear that the investigative technique contemplated engages a high level of privacy; one that is even higher than when the contents of a device can be accessed without the compelled participation of the suspect. As put by Michael Froomkin as early as 1999, encryption changes one's reasonable expectation of privacy by augmenting it.[1367] By compelling someone to decrypt a device or data, law enforcement is

[1364] *Ibid* at para 53.
[1365] *Spencer*, *supra* note 241.
[1366] *Ibid* at para 50.
[1367] A Michael Froomkin, "The Constitution and Encryption Regulation: Do We Need a 'New Privacy'?" (1999) 3:1 NYU J Legis & Publ Pol'y 25 at 31.

seeking to access the evidence, but also to link a suspect with that same evidence, in order to support prosecution. What distinguishes compelled decryption from the power to search or seize the device itself is the self-incrimination aspect of the decryption act. The passivity that searches and seizures normally entail is removed as decryption necessitates an active act by the suspect, literally in assistance of the state's investigation.

Granting law enforcement the power to decrypt without prior authorization would unduly affect privacy on a wider level, by implicitly stating that individuals do not have privacy against the state, or should not worry about the state abusing its powers. As stated by Penney and Gibbs, not recognizing the existence of a reasonable expectation of privacy towards the subject matter of a compelled decryption order would be highly problematic, as it would grant law enforcement the power "to demand key disclosures from suspects without any evidence connecting them to the encrypted data."[1368] If this was the case, the preventative aspect of s. 8 would be seriously undermined.

To be clear, encryption does not give the suspect the right to expect that the government will not try to access the decrypted data by other means, by using one of the other available "encryption workarounds,"[1369] within was is reasonable under the *Collins* analysis,[1370] nor does it mean that individuals who do not encrypt their data or devices lose all reasonable

[1368] Penney & Gibbs, *supra* note 3 at 243.

[1369] Geshowitz, *supra* note 1239 at 1147; Penney & Gibbs, *supra* note 3 at 216; Orin S Kerr, "The Fourth Amendment in Cyberspace: Can Encryption Create a Reasonable Expectation of Privacy?" (2001) 33:2 Conn L Rev 503 at 517–518. In this article, Kerr argues that the Fourth Amendment does not provide additional privacy protections for encrypted data (versus non-encrypted data). As such, once legally in the hands of law enforcement, data can be decrypted without further implication of the Fourth Amendment. In the scenario that law enforcement is not trying to compel assistance from the suspect, this would also be the case in Canada, under the approach suggested in this thesis.

[1370] *Collins*, *supra* note 31 at 278.

expectation of privacy.[1371] The difference here lies in the compelled act of decryption, which modifies the self-incrimination and privacy interests of the suspect. Without the coercive aspect of compelled decryption, the current applicable framework when it comes to privacy in digital data is sufficient to mitigate the infringement on privacy caused by law enforcement's access to the data. This is why a reconciled approach to ss. 7 and 8 is required in the context of compelled decryption and why the reasonableness of a compelled decryption power will rest on the existence of strict pre-conditions made applicable by a prior authorization provision.

It could be argued that if encryption raises privacy considerations in such an important way, law enforcement should not be allowed to try to circumvent the encryption altogether, even without resorting to compulsion, by using the other "encryption workarounds." However, this interpretation would stretch the ambit of the relevant *Charter* protections in an unprecedented and unsupported way. While encryption is indeed an important assertion of privacy on digital data, once the self-incrimination aspect of compelled decryption is removed encryption should not serve as a method to create an inviolable sphere of privacy. That would be inconsistent with the fact that *Charter* protections are not absolute, and that law enforcement is allowed to conduct *reasonable* searches and seizures. It is also doubtful that Parliament would want to extend the protection given to encryption in such a way, as it would impede criminal investigations in an important way.[1372] That being said, it is very well possible that

[1371] This would be inconsistent with the fact that risk analysis was rejected by the SCC in *Duarte*, *supra* note 607. See also *Marakah*, *supra* note 260 at para 41; *Cole*, *supra* note 30 at para 54.

[1372] As noted before, Parliament can always decide to go above and beyond the minimal protections granted by the *Charter*. However, in this situation, it is very unlikely that this would be seen as a viable policy decision, due to the impact that this would have on criminal investigations throughout Canada.

some of the "encryption workarounds" would not respect the *Collins* analysis.[1373] This is especially true when it comes to lawful hacking and its various applications that can be highly invasive. However, it is premature to engage in this analysis at this point, due to the very limited information regarding the use of lawful hacking as an investigative tool in Canada up to this day.[1374]

Because the SCC has recognized that the principle against self-incrimination is linked with the protection of privacy,[1375] it is possible to recognize that compelled decryption engages significant privacy interests, alongside the more obvious self-incrimination interests. As mentioned previously, if the SCC so easily recognized that personal digital data is private, it would surely recognize that encryption enhances that privacy expectation, as it effectively secures data from unwanted intrusion. Encryption, after all, is designed to keep data secure, whether at rest or in transit. Further, if we do not recognize an increased expectation of privacy towards encryption and the act of decryption, compelled decryption would be available to the authorities with the only condition that immunity is given towards the act of decryption, as it alleviates the self-incrimination aspects of decryption and reflects the traditional balance between testimonial and non-testimonial self-incrimination.[1376] This seems too weak a protection considering the strength of self-incrimination and privacy interests at stake, in the unique context of compelled decryption.

[1373] This would most likely be problematic under the second and third step of the *Collins* test. See *Collins*, *supra* note 31 at 278.
[1374] This might, however, change rapidly, as the Privacy Commissioner of Canada is investigating the use of lawful hacking by the RCMP. See Section 7.3.1(B)(i) *infra*.
[1375] See Section 7.1.1(A) *supra*.
[1376] See Section 7.3.1(E) *infra*.

B) The Reasonableness of the Search or Seizure

The conclusion that compelled unlocking of devices involves a reasonable expectation of privacy triggers s. 8 of the *Charter* and brings us to the second stage of the analysis, which is the determination of whether this investigative power can be reasonable under the three-step approach dictated by *Collins*.[1377]

i. Presence of a Lawful Authorization

No generally recognized common law power grants the authorities a general power to compel decryption. While the power of search incident to arrest allows law enforcement to conduct the search of an electronic device under specific conditions,[1378] compelled decryption is different as it entails the coerced participation of the accused. Accordingly, the ancillary powers doctrine must be applied to determine whether the common law should be interpreted to allow for such a power.

On the first step (i.e., whether "the police were acting in the course of their duty, when they effected that interference"[1379]), compelled decryption is linked to the investigative duties that are incumbent upon law enforcement.[1380] Compelled decryption can indeed be an interesting tool in law enforcement's arsenal of investigative techniques, especially considering its low cost and high efficiency (as opposed to other "encryption workarounds"). Accordingly, the first step of the ancillary powers doctrine is met. On the second step of determining whether

[1377] *R v Collins*, *supra* note 31 at 278.
[1378] *Fearon*, *supra* note 1 at para 83.
[1379] *Godoy*, *supra* note 620 at para 7.
[1380] It is uncontroversial that law enforcement has the duty to solve and prevent crimes. See *inter alia Kang-Brown*, *supra* note 229 at para 52; *Fleming v Ontario*, *supra* note 619 at para 69.

the "conduct of the police did not involve an unjustifiable use of powers in the circumstances,"[1381] it must be determined whether the "police action is reasonably necessary for the fulfillment of the duty."[1382] Three factors were set out by the majority in *MacDonald* to answer this question:

1. the importance of the performance of the duty to the public good;
2. the necessity of the interference with individual liberty for the performance of that duty; and
3. the extent of the interference with individual liberty.[1383]

While accessing evidence in a readable state is important to the performance of investigative duties and investigating crimes is an important police duty in itself (1st *MacDonald* factor), compelled decryption is only necessary in specific cases where no other "encryption workaround" is available to law enforcement (2nd *MacDonald* factor). However, law enforcement officials will not be aware of the need to use compelled decryption until they try other "encryption workarounds," and many of them require time and effort to be deployed by experts with specialized training. Thus, the time required to attempt to use other "encryption workarounds" removes the temporal necessity of allowing law enforcement to act without a warrant, as it will allow law enforcement to seek and obtain a judicial authorization. Accordingly, it is not "reasonably necessary"[1384] to grant law enforcement the power to

[1381] *Godoy*, *supra* note 620 at para 7.
[1382] *Fleming v Ontario*, *supra* note 619 at para 47, referring to *MacDonald*, *supra* note 647 at para 36.
[1383] *MacDonald*, *supra* note 647 at para 37 (references from the original omitted). The dissent in this case (per Rothstein, Moldaver and Wagner JJ.) did not pertain to the ancillary powers doctrine, but to the proper interpretation of *Mann* and the standard applicable to safety searches. The three factors were also referred to by the SCC in *Fleming v Ontario*, which is a unanimous decision.
[1384] *MacDonald*, *supra* note 647 at para 36.

compel decryption without a warrant, during the course of regular investigations.[1385] Further, the strength of the privacy and self-incrimination interests present and the extent to which compelled decryption interfere with individual liberty outweighs the importance of granting such warrantless power to law enforcement (3rd *MacDonald* factor). Consequently, a warrantless compelled decryption power does not satisfy the second sept of the ancillary powers doctrine and should not be recognized to law enforcement.

Further, it will not always be appropriate for the courts to "expand common law rules, in order to address perceived gaps in police powers."[1386] It is generally preferrable to leave to Parliament the decision to extend police powers,[1387] especially in circumstances where the obtention of a prior judicial authorization would not unduly restrict law enforcement in their aim to investigate and prevent crimes. It should also be remembered that *Hunter* generally supports the prior judicial authorization requirement.[1388] Requiring a court order to be

---

[1385] The only caveat to this would possibly be in exigent circumstances, where the temporal necessity of accessing evidence in a decrypted state is increased.

[1386] *Kang-Brown*, *supra* note 229 at para 6 (as per LeBel J.'s dissenting motives). See also *Fleming v Ontario*, *supra* note 619 at para 4, referring to *Wong*, *supra* note 567 at 57. While this was not recognized by the majority in *Kang-Brown* and indeed multiple SCC decisions have expanded police powers, this is generally criticized. See Patrick Healy, "Investigative Detention in Canada" (2005) Crim LR 98 and James Stribopoulos, "In *Search* of Dialogue: The Supreme Court, Police Powers and the *Charter*" (2005) 32 Queen's LJ 1 (both cited in *R v Clayton*, 2007 SCC 32, [2007] 2 SCR 725 at para 74). See also James Stribopoulos, "Sniffing Out the Ancillary Powers Implications of the Dog Sniff Cases" (2009) 47 SCLR: Osgoode's Annual Constitutional Cases Conference 35 at 45-46, where he states that:

> "Historically, when it came to government interfering with individual liberties, our courts were very reluctant to use their law-making authority to expand state powers. In fact, in this context, the common law courts traditionally showed much restraint. That restraint eventually became the bedrock of English constitutional law, taking the "principle of legality" as its label. Applying that principle, common law courts have long insisted that any interference with individual liberty or property rights be premised on clear legal authority. Absent such authority, the common law erred on the side of individual freedom. It is in this sense that the common law has been viewed, in the words of LeBel J. as the "law of liberty"." (Reference from the original omitted.)

[1387] *Wong*, *supra* note 567 at 56–57.

[1388] *Hunter*, *supra* note 31 at 160.

obtained prior to compelling a suspect to decrypt a device or data ensures that some judicial control of law enforcement will remain.[1389]

The *Criminal Code* does not currently contain a provision specifically tailored for compelled decryption. As previously mentioned, courts have concluded that neither a s. 487 search warrant,[1390] a s. 487.092 impression warrant,[1391] nor a s. 487.02 assistance order[1392] could be used in such manner. Further, neither the *Identification of Criminals Act*[1393] nor s. 487.05 of the *Criminal Code* are applicable in the context of compelled decryption of data secured by biometric authentication methods because the objective of these provisions is to identify criminals by using their fingerprints or bodily substances, not to discover evidence.

The general warrant provision found in s. 487.01 of the *Criminal Code* probably comes closest to allowing compelled decryption. Indeed, the provision was adopted specifically to allow the use of innovative investigative techniques when no other provision is applicable.[1394] The provision can appear appropriate to allow compelled decryption for three main reasons. First, s. 487.01(3) specifically allows the issuing judge to consider imposing any terms and conditions to make sure that the search or seizure is reasonable in the circumstances, which could ensure that the warrant is tailored to the specific situation under investigation. Second, compelled decryption does not interfere with bodily integrity, even when it comes to biometric authentication measures, thus respecting s. 487.01(2). Third, before issuing the general warrant, the issuing judge must be satisfied that the use of the proposed technique is

[1389] Jaffer & Rosenthal, *supra* note 101 at 302.
[1390] *R c Boudreau-Fontaine*, *supra* note 779.
[1391] *Impression Warrant Application (Re)*, *supra* note 1180.
[1392] *R v Shergill*, *supra* note 230; *R v Talbot*, *supra* note 1179.
[1393] *Identification of Criminals Act*, *supra* note 820.
[1394] *Criminal Code*, *supra* note 37, s 487.01(1)(c); *TELUS*, *supra* note 249 at para 20.

in the best interests of the administration of justice, following s. 487.01(1)(b). Accordingly, the general warrant provision is arguably available to law enforcement in order to compel decryption.

However, the strength of the privacy and self-incrimination interests at play strongly militate for the creation of a separate order that would prescribe conditions better suited to the unique context of encryption. Except in a few rare cases,[1395] the general warrant provision seems to have only been used in situations where accused individuals are not forced to participate in an investigation that concerns them.[1396] This seems to stretch the ambit of the general warrant farther than Parliament meant it to go. Consequently, the use of the general warrant in the context would not respect the second step of the *Collins* test, as it would be an unreasonable use of this investigative tool.

ii. Reasonableness of the Law Itself

The determination of whether a law is reasonable entails examining the state's objectives in relationship with the individual rights being triggered by the contemplated search or seizure power.[1397] Finding the balance between these polarities is the keystone of creating a compelled decryption framework that respects the second prong of the *Collins* test, as well as the imperatives put forth by s. 7 of the *Charter*. Once combined, ss. 7 and 8 indeed allow to

[1395] See for example *R v H-G (R)*, *supra* note 785 and *R v H (TG)*, 2014 ONCA 460. However, in both these cases the general warrant provision was used to view and photograph an intimate part of the suspects' bodies, which is arguably very different from forcing a suspect to unlock a device or decrypt data, due to the information that action gives access to.
[1396] Coughlan, *supra* note 799 at 215–229.
[1397] *Rodgers*, *supra* note 631 at para 27.

draw a strong inference that judicial authorization is necessary when it comes to compelled decryption.

In light of new surveillance powers propelled by digital technologies, such as Big Data analytics, facial recognition, and predictive policing technologies, it has been suggested that the "going dark" phenomenon and its attendant dangers have been overstated, as we now live in a surveillance society.[1398] Encryption, then, does not only augment our privacy expectations but does so in a way that is proportionate with the state's rising surveillance powers. Contrary to what some say, encryption does not tip the scale in favor of criminals; rather it ensures that some level of individual privacy remains.[1399] Why then would law enforcement need a compelled decryption power if encryption is simply a way of reasserting privacy in a digital world?

The answer to this question lies in the strength of encryption. It has been said that "encryption holds the promise of absolute privacy,"[1400] which is an obvious challenge to law enforcement's ability to investigate crimes in situations where encryption is deployed in such manner as to completely block an investigation. In those cases, compelling the person under investigation will possibly be the only way of accessing the decrypted data.[1401]

[1398] See *inter alia* Gill, *supra* note 3 at 452–453; Hurwitz, *supra* note 69 at 400; Czerniawski & Boyack, *supra* note 298 at 90.

[1399] As put by Michael Froomkin, "The Metaphor is the Key: Cryptography, The Clipper Chip, and the Constitution" (1995) 143 U Pa L Rev 709, referred to in Babiarz, *supra* note 1354 at 358, encryption (rather than encryption regulation) seeks to return to the *status quo* of law enforcement access to communications, by ensuring that some communications remain private, like the conversations that we previously had in an open field.

[1400] Ungberg, *supra* note 38 at 548. See also McGregor, *supra* note 6 at 599.

[1401] Lemus, *supra* note 220 at 544.

Recognizing an absolute right to privacy enforced by encryption is contrary to our understanding of privacy, both under s. 8 of the *Charter* and more generally.[1402] The creation of an inviolable zone of privacy is not desirable for society as a whole, as it can be used to hide unlawful behaviours and wrongdoings, especially considering that digital evidence is now increasingly prevalent.[1403] Some cases, such as many of those involving digitized child pornography, will simply founder if decryption is unavailable; this is arguably a high cost for society to bear. It can also be seen as contrary to the rule of law to allow individuals rights to obstruct a lawfully authorized search,[1404] considering that without encryption the plaintext would have been easily accessible to the state. The reasonableness aspect of s. 8 is what is necessary to attain a balance between these polarities. While refusing to recognize a reasonable expectation of privacy in encryption and the data it protects would have tipped the scale too heavily in favor of the state, refusing to create a compelled decryption power tips the scale too heavily in favor of the suspects and accused individuals.

Providing law enforcement with compelled decryption powers allows for strong encryption to remain available to law abiding citizens, while not disproportionately protecting criminals.[1405] This recognizes the positive aspects of encryption, which also need to be considered when balancing the opposed interests at play. This is perhaps another way encryption challenges our understanding of reasonable search and seizure powers, as the constitutional analysis needs to incorporate the fact that encryption is not only an impediment to the state, but also something from which the state benefits.

[1402] Gray, *supra* note 1272 at 637; Bales, *supra* note 943 at 1309.
[1403] Terzian, *supra* note 231 at 310.
[1404] Hayes, *supra* note 339 at 12.
[1405] Hill-Smith, *supra* note 150.

To be fair, in some situations encrypted data will still remain out of law enforcement's reach. Deniable encryption,[1406] the use of cloud computing on platforms that will be unknown to police officers, as well as a refusal by a suspect to comply with a decryption order, will all impede access to data in a form that is relevant to a criminal investigation. However, this has always been the case. Some information has always been out of the reach of the long arm of the law. What would be unacceptable when focusing on balancing the opposed interests at play would be to remove all encrypted data from law's reach, or conversely to grant compelled decryption powers in such way that digital privacy is rendered a meaningless concept.

Strong privacy interests will warrant severe conditions being put in place in order for law enforcement to use a specific investigatory power.[1407] Because compelled decryption raises self-incrimination considerations that are not present when law enforcement is seeking to search unprotected devices, additional conditions are required to adequately balance the opposed interests at play.[1408] The specific conditions required in order for a compelled decryption framework to be valid under ss. 7 and 8 of the *Charter* are proposed in section 7.3 *infra*.

[1406] Sacharoff, *supra* note 20 at 222.

[1407] *Gomboc*, *supra* note 291 at para 20; *Simmons*, *supra* note 490 at 517. See Section 5.1.3 *supra* and Moore, *supra* note 240 at 209–213.

[1408] See for example *Golden*, *supra* note 641, in which the SCC concluded that the higher privacy interests present when police are conducting strip searches requires a modification of the search incident to arrest framework. See also *TELUS*, *supra* note 249 at para 73, where Cromwell J. states that "Part VI alone imposes several further requirements [when compared to the general warrant provision] in the interest of protecting the right to privacy."

iii. Manner in which the Search of Seizure is Carried Out

Finally, the third step of the *Collins* analysis requires a highly contextual examination of whether a search or seizure was carried out in a reasonable way, under the specific circumstances that took place in the case being examined. For this reason, it is premature to engage in an analysis under this rubric.

7.3 Suggested Approach to Compelled Decryption of Data or Unlocking of a Device by a Suspect

As suggested in the introduction to this thesis, a compelled decryption framework should respect five general principles: (1) Parliament should be **proactive** and create a framework, rather than leaving it up to the courts; (2) the framework needs to be **coherent**; (3) the framework should be **balanced**, which is what has been considered in the previous section; and (4) it should be **adaptable**, reflecting the idea that technological advancements are hard to predict.

Requiring Parliament to intervene to create a compelled decryption power is consistent with the idea that courts are currently ill-equipped to develop an appropriate framework applicable to encryption. Courts are limited by the adversarial nature of our justice system, which functions on the evidence that is adduced by the parties.[1409] Legislative intervention is preferable in this field because it would allow for the consultation of experts that could provide Parliament with different perspectives, both legally and technologically.

[1409] Fehr, *supra* note 319 at 69, 97. See also Justice Karakatsanis' dissenting reasons in *Fearon*, *supra* note 1 that recognizes that the Court did not receive sufficient information on the question of passwords.

Having been presented with all the relevant information, Parliament would be in a better situation to create a holistic compelled decryption framework, one that has better chances to survive the test of time. For example, it seems that if the SCC had refused to expand the doctrine of search incident to arrest to electronic devices in *Fearon*,[1410] Parliament would probably have addressed the issue of password-protected devices when creating a provision on this subject.[1411] Further, a clear framework created by Parliament would also remove some of the discretionary interpretation that comes from leaving this issue to be decided by the courts.[1412] It would also address the fact that courts can only tackle these issues *ex post*, which does little to satisfy the preventative aspect of s. 8 of the *Charter*.[1413]

The Ontario Court of Justice in *Re Impression Warrant Application (487.092)* based its decision mostly on the fact that this provision was not adopted with the intent of allowing the collection of fingerprints to give access to data.[1414] In *Shergill*, the Court specifically mentioned that legislative action could provide a different approach to the issue of compelled decryption.[1415] Both these comments by the courts—one as part of the *ratio decidendi*, one in *obiter dictum*—provide incentive for Parliament to consider adopting a framework on this subject.[1416]

[1410] *Fearon*, *supra* note 1.

[1411] See generally Colton Fehr & Jared Biden, "Divorced from (Technological Reality): A Response to the Supreme Court of Canada's Reasons in *R. v. Fearon*" (2015) 20 Can Crim L Rev 93; Hayes, *supra* note 339, on how *Fearon* has failed as a decision because it did not consider the impact of password and biometric authentication methods.

[1412] Zarefsky, *supra* note 331 at 191.

[1413] Fehr, *supra* note 319 at 97.

[1414] *Impression Warrant Application (Re)*, *supra* note 1180 at para 14.

[1415] *R v Shergill*, *supra* note 230 at para 51.

[1416] Hochstrasser, *supra* note 1096 at 23.

7.3.1 Conditions Applicable to the Issuance of a Compelled Decryption Authorization

As mentioned, the strength of the privacy and self-incrimination interests at play dictate that stringent pre-conditions to the issuance of a compelled decryption authorization should be put in place.

It is worth stating at this point that the proposed framework found below is strictly a decryption power, not a search or seizure power, such as what has been done in the UK with s. 49 of *RIPA* and in Australia under various federal and provincial acts. As such, law enforcement still needs to respect the general pre-conditions to lawfully obtain the right to search a specific digital device, usually by obtaining a s. 487 search warrant.[1417]

A) The Right to Remain Silent is Absolute

Canadian criminal law places great importance on the accused's right to remain silent. No *Criminal Code* or common law power allows law enforcement to compel a suspect to make declarations, as this would infringe the principle against self-incrimination. The interdiction of compelling a suspect to reveal information verbally weighed heavily in *Boudreau-Fontaine*[1418] and *Shergill*.[1419] In both instances, the courts concluded that the accused's right to remain silent had been breached by the obligation to reveal his password. In furtherance of this principle, it is also accepted that the silence of the accused cannot be used against them

[1417] Absent exigent circumstances which would make s. 487.11 of the *Criminal Code* applicable, compelled decryption powers should be unavailable as accessory to a search incident to arrest because the proposed framework rests on the pre-condition that no other "encryption workaround" is available to law enforcement. Thus, law enforcement would not be able to respect the timing condition of the search incident to arrest doctrine, making the use of a search warrant necessary.
[1418] *R c Boudreau-Fontaine*, *supra* note 779 at para 39.
[1419] *R v Shergill*, *supra* note 230 at paras 21–23.

to prove guilt beyond a reasonable doubt.[1420] The only possible nuance to this statement is that once the Crown has established a case to meet, the silence of the accused at trial can result in a declaration of guilt.[1421]

In order to respect this strong constitutional protection against coerced statements, a framework allowing for compelled decryption should not allow law enforcement to compel a suspect to reveal a passcode or encryption key directly to the authorities, either by stating it out loud, writing it down, or showing the swipe-pattern to the police. Rather, law enforcement should only be allowed to compel a suspect to unlock a device or decrypt data by inputting the key, passcode, or pattern themselves, directly into the device or encryption software, in a manner where law enforcement does not obtain the passcode. This is similar to what is done in the UK, where law enforcement's primary power to compel decryption is truly a power to obtain the plaintext of the sought-after data.[1422] The proposed compelled decryption power then is more akin to a search than a seizure.[1423]

This approach is justified under two rationales. First, it ensures that the suspect's right to remain silent (under s. 7 of the *Charter*) is not breached. Even though the act of decryption still carries the same testimonial qualities related to ownership and control over the plaintext (which are addressed by granting act of decryption immunity to the suspect, see *infra*), it better reflects the traditional divide between what is acceptable *versus* what is not acceptable when it comes to coercive investigative techniques, as distinguished between testimonial and

[1420] *Noble*, *supra* note 482 at para 46.
[1421] *Darrach*, *supra* note 388 at para 54; *P (MB)*, *supra* note 367 at 579; *Dubois*, *supra* note 360 at 357.
[1422] See Section 6.3.2(A) *supra*.
[1423] While this thesis generally avoids using analogies and comparisons with "real world" items (see Section 2.7 *supra*), it is tempting here to use the analogy that compelled decryption requires a suspect to unlock the door, not hand over the keys.

non-testimonial self-incrimination. For example, a driver can be intercepted and required to comply with various sobriety tests (which are incriminating) but cannot be forced to verbally state if he has consumed alcohol before taking the wheel.[1424] This does not contravene the right against self-incrimination, because of the limited use that can be made of the self-incriminating evidence obtained by compulsion.[1425] Likewise, the SCC in *SAB* unanimously determined that the compelled production of samples for DNA testing did not violate the protection against self-incrimination, due to the strict requirements applicable to DNA search warrants.[1426] Second, it ensures that law enforcement will not save the passcode and try to use it to access data related to the suspect that could be found on other devices or other platforms, whether during the same investigation or a subsequent one, which further mitigates the risks of abuse of power by the state.[1427]

A note on Martin J.'s approach in *Mills II* is required here. In her reasons, she concludes that the fact that electronic communications platforms make permanent recordings of our communications by nature should not change the normative privacy expectation that the state will not invade our private conversations at will.[1428] This makes sense: if as a society we are unwilling to allow the state to invade our private conversation and make permanent recordings of them without prior authorization, the fact that electronic communications technology have fundamentally changed how we communicate should not be used to lessen our privacy

[1424] Law enforcement is, however, allowed to ask this question. See *Orbanski*, *supra* note 442.
[1425] *Orbanski*, *supra* note 442; *R v Thompson*, 2001 CanLII 24186 (ON CA).
[1426] *SAB*, *supra* note 430 at para 59.
[1427] This would be especially problematic considering the high proportion of users that recycle their passwords. See Macy Bayern, "Why 72% of people still recycle passwords", (18 July 2019), online: *TechRepublic* <https://www.techrepublic.com/article/why-72-of-people-still-recycle-passwords/#:~:text=Users%20recycle%20the%20same%20password,to%20a%20Security.org%20report.>.
[1428] *Mills II*, *supra* note 264 at para 90.

protections, even though our communications are now automatically recorded by the technology we use.

When applied to encryption, this would most likely mean that the fact that encryption keys or passcodes have a physical or material manifestation (i.e., they can be *physically* inputted in the device) should not be used to lessen the protection offered to encryption. Effectively, this would mean that inputting a passcode into a device should receive the same protection as stating that passcode verbally. Under the approach suggested here, this would mean that compelled decryption should never be allowed.

This interpretation would be unsatisfactory when considering the overarching goal of s. 8, which is to prevent *unreasonable* searches and seizures and to reconcile the opposed interests at play. Accepting this as the applicable minimal protection would effectively create an inviolable sphere of privacy (due to the nature of encryption), which is simply inconsistent with the SCC's jurisprudence on privacy. It also fails to recognize that the protection against self-incrimination allows for compelled statements in some situations. Further, it should be kept in mind that Martin J.'s reasons in *Mills* do not represent the current state of the law in Canada, as she was not only dissenting, but also the only one to do so.

However, this option is something Parliament could decide to follow if it concludes that this is the policy orientation it wants to follow. As mentioned, Parliament can always decide to go above and beyond the minimal protections set forth in the *Charter*. The *Charter* considerations are not the only factors to be considered for policymakers. For example, Gill, Israel, and Parsons have included a list of factors in their examination of the encryption

debate.[1429] Not all these factors relate to the minimal protection created by ss. 7 and 8 of the *Charter*.

B) Compelled Decryption is Only Available When no Other Encryption "Workaround" is Reasonably Applicable, for Offences of Sufficient Seriousness, and When in the Best Interest of the Administration of Justice

As previously mentioned, compelled unlocking should only be available when no other "encryption workaround" can reasonably be employed by the authorities, whether because of time or technological constraints. This investigative necessity criterion reflects the idea that exceptional powers should only be granted in the presence of exceptional circumstances.[1430] An investigative necessity requirement already exists in the *Criminal Code* when it comes to the interception of private communications.[1431] As such, the text of s. 186(1)(b) of the *Criminal Code* could provide inspiration when it comes to drafting this requirement. An investigative necessity condition has been included in the UK under *RIPA*,[1432] and in the legislation adopted in Victoria and Queensland, in Australia.[1433]

Investigative necessity requirements are useful to strike the appropriate balance between individual and societal rights.[1434] While they are not required in every scenario involving privacy rights,[1435] the enhanced privacy interests linked to compelled decryption would make

[1429] Gill, Israel & Parsons, *supra* note 3 at 40.
[1430] Cambrea Beller, "Unlocking Your Phone Could Lock you up: Say Your Goodbyes to the Right against Self-Incrimination" (2020) 55:1 New Eng L Rev 27 at 43.
[1431] See Section 5.3.3 *supra*.
[1432] *Regulation of Investigatory Powers Act 2000*, *supra* note 1012, s 49(2)(d).
[1433] Hochstrasser, *supra* note 1096 at 33–34.
[1434] *Araujo*, *supra* note 642 at para 22.
[1435] *SAB*, *supra* note 430 at paras 53-54.

this requirement necessary in order to respect s. 7 of the *Charter*. In the case of compelled decryption, the whole premise of granting this power to law enforcement rests on the assumption that encryption can unduly obstruct a lawful investigation. If this is not the case in a specific investigation, why grant this power to law enforcement in the first place? This requirement would also address concerns that powers to compel decryption are merely convenient, not truly necessary, or that encryption is not truly as insurmountable as it may seem.[1436]

Further, as mentioned by Justice Arbour (writing for a unanimous court) in *SAB*, the investigative requirement found in s. 186(1)(b) of the *Criminal Code* is justified by the fact that wiretaps "are sweeping in their reach [and will] inevitably intrude into the privacy interests of third parties who are not targeted by the criminal investigation."[1437] This is also the case when it comes to compelled decryption as it will give law enforcement access to private data that inevitably concerns innocent third parties.

Imposing such an investigative necessity requirement also has the advantage of addressing the issue of future unforeseen changes in encryption and decryption technology. On one side, advancements in the strength of encryption could render the other "encryption workarounds" impossible to apply. For example, it has been suggested that quantum computing holds the possibility of strengthening encryption even further, making encryption more difficult to circumvent in general.[1438] On the other side, advancements in hacking techniques could also

[1436] Diab, *supra* note 3 at 284; Gill, Israel & Parsons, *supra* note 3 at 80; Parsons, *supra* note 56; Terzian, *supra* note 231 at 311–312.
[1437] *Ibid*. at para 54.
[1438] Olivia Gonzalez, "Cracks in the Armor: Legal Approaches to Encryption" (2019) 2019:1 U Ill JL Tech & Pol'y 1 at 22–23.

make it unnecessary to resort to the suspect's participation to decrypt data. Conversely, quantum computing could also make it possible to crack encryption using a brute force attack in a fraction of the time it currently takes.[1439]

Digital evidence is now relevant in almost every investigation, from smaller crimes to more sophisticated criminal schemes. Encryption has consequently the potential to hinder virtually every investigation. However, the significant intrusion on privacy that follows compelled decryption dictates that a compelled decryption power should not be used in every investigation, even when no other "encryption workaround" is applicable. Two requirements should be used to make sure that the heightened privacy interests present are respected. First, Parliament should limit the use of the authorization to a list of infractions of more serious nature, as is done for wiretap authorizations. These offences might not be the exact same as the ones found in s. 183 of the *Criminal Code* but compelled decryption should not be available for petty crimes. Second, Parliament should impose a requirement that the issuance of the authorization is in the best interests of the administration of justice, like what is done under the general warrant provision and for wiretap authorizations.[1440] As described in *Duarte*, the best interest requirement "imports as a minimum requirement that the issuing judge must be satisfied that there are reasonable and probable grounds to believe that an offence has been, or is being, committed and that the authorization will afford evidence of that offence."[1441] These requirements would ensure that the intrusiveness of the technique is

[1439] For a definition of quantum computing and how it may affect encryption, see Amit Katwala, "Quantum computing and quantum supremacy, explained", (5 March 2020), online: *Wired* <https://www.wired.co.uk/article/quantum-computing-explained>.
[1440] For example, in *R v Pratchett*, *supra* note 176 the prosecution was able to secure a conviction even though the accused's computer could not be decrypted. While this may not always be the case, it stands for the proposition that compelled decryption is not always required, even when no other "workaround" is applicable.
[1441] *Duarte*, *supra* note 607 at para 24.

adequately balanced with the importance of the evidence, in relation to the gravity of the alleged offence, and the strength of the privacy and self-incrimination interests at play.

Alternatives to compelled decryption include: using security cameras to view the suspect's passcode;[1442] using surveillance to witness the swipe pattern used to unlock a phone;[1443] using the gyroscopic function of an iPhone to decipher the key;[1444] using a dynamic entry to prevent the suspect from deleting relevant data;[1445] finding the password noted on a piece of paper or elsewhere;[1446] using a key-logger (i.e., a software usually used by hackers to know what keys are used on a specific device) to obtain the suspect's passwords;[1447] or by using the exigent circumstances doctrine to search a device that is in a decrypted state.[1448] What these techniques have in common is that they do not require the compelled participation of the accused, making s. 7 of the *Charter* inapplicable, even though many of these require some type of judicial authorization under s. 8 of the *Charter*. As such, these alternatives should always be given priority by law enforcement, as they will not implicate the right against self-incrimination and the heightened privacy interests implicated when an individual is compelled to unlock a device or decrypt data.

i. 'Lawful Hacking' as an Alternative to Compelled Decryption

Even with the existence of a compelled decryption power or other "encryption workarounds," it could still be preferable in some situations for investigators to access data remotely. In some

[1442] *Wu c R*, 2019 QCCA 1702.
[1443] *R v Crawley*, 2018 ONCJ 394.
[1444] van den Hoven van Genderen, *supra* note 256 at 349.
[1445] *R v Burke*, *supra* note 747.
[1446] *R v Nero*, *supra* note 1161 at para 153.
[1447] Colarusso, *supra* note 6 at 96.
[1448] *R v Hart*, *supra* note 843.

cases, this will be possible with the help of the TPDC,[1449] while in other cases lawful hacking techniques can be used. As seen previously in Chapter 6, lawful hacking is defined as the use by the government of techniques usually employed by hackers for investigatory purposes, including to circumvent encryption, whether employed to protect data at rest or data in transit.[1450] It can also be used to identify individuals using "onion routing" services, such as TOR, to access the dark web.[1451]

Lawful hacking can be used by law enforcement agencies without recruiting the help of the TPDC, by exploiting existing vulnerabilities in devices and software.[1452] It involves a four-step approach of (1) delivering the malware to the target; (2) exploiting the identified vulnerability; (3) executing the attack (i.e., collecting the sought-after information); and (4) reporting the information back to the government-controlled server.[1453] Lawful hacking functions on the presence of a vulnerability in the targeted device's (or internet-based service's) security system, making this "encryption workaround" contingent on the existence of a unpatched vulnerability.[1454] It can also rely on "social engineering," which uses the

[1449] See Chapter 8.

[1450] Gonzalez, *supra* note 1438 at 27–28. See also Aucoin, *supra* note 147 at 1443–1448 for examples where lawful hacking was used by the US government to conduct investigations.

[1451] TOR, or "The Onion Router", is a service allowing users to access the dark web (which is a part of the deep web, the un-indexable part of the internet that cannot be accessed with traditional search engines) anonymously by first providing software, and second by providing a network of volunteer computers that allow that software to function and obfuscate the IP address and location of the users. The term "onion routing" comes from the multiple layers of routing created by such software. See Aucoin, *supra* note 147 at 1439–1440. Lawful hacking is said to be the only way to identify people using TOR to hide their criminal activities on the dark web. Paul Ohm, "The Investigative Dynamics of the Use of Malware by Law Enforcement" (2017) 26:2 Wm & Mary Bill Rts J 303 at 304.

[1452] Rafita Ahlam, "Apple, the Government, and You: Security and Privacy Implications of the Global Encryption Debate" (2021) 44:3 Fordham Int'l LJ 771 at 795–796.

[1453] Jonathan Mayer, "Government Hacking" (2017) 127:3 Yale LJ 570 at 583–589.

[1454] Ohm, *supra* note 1451 at 312. However, because code is never perfect, there will usually be vulnerabilities to be exploited, at least temporarily until a patch is issued by the vendor AND applied by the user.

naivety of the target to get them to install or otherwise download the malware used to conduct the attack, instead of using purely technological means.[1455] It is important to note that the use of these techniques can constitute an offence under ss. 342.1, 342.2, and 430(1.1)(5) of the *Criminal Code* if done without previously obtained judicial authorization.

Currently, no court authorization is specifically applicable to the use of lawful hacking techniques in Canada, contrary to what is done in the UK and elsewhere in the world.[1456] As such, the most appropriate authorization would be a s. 487.01 general warrant, as the use of these techniques involves intruding upon a reasonable expectation of privacy, considering law enforcement is seeking access to a suspect's devices or data or is trying to monitor their online activities.[1457] If the specific lawful hacking technique used also gives law enforcement access to private communications in real time, then a wiretap authorization should also be obtained prior to the deployment of the technique.[1458] Lawful hacking can involve highly specialized techniques and may not be appropriate in all circumstances, due to the expertise required, the

[1455] Rachel Bercovitz, "Law Enforcement Hacking: Defining Jurisdiction" (2021) 121:4 Colum L Rev 1251 at 1259. "Social engineering" can be defined as "the act of manipulating a person to take action that may or may not be in the 'target's' best interest." See Christopher Hadnagy, *Social engineering: the art of human hacking* (Indianapolis, IN: Wiley, 2011).

[1456] See *inter alia* Ahlam, *supra* note 1452.

[1457] West & Forcese, *supra* note 85 at 18; Dheri & Cobey, *supra* note 77 at 28; Christianson, *supra* note 1312 at 264; Ohm, *supra* note 1451 at 327; Mayer, *supra* note 1453 at 614; Jason Lebowitz, "Technology and Individual Privacy Rights: The Fourth Amendment Implication of Exploiting Zero-Day Vulnerabilities for Domestic Investigations" (2015) 47:1 Colum Hum Rts L Rev 242 at 257. The existence of a reasonable expectation of privacy triggering the application of s. 8 of the Charter is not as clear when the lawful hacking technique is used to obtain the suspect's IP address, as this information can usually be obtained without a warrant by law enforcement, for example by conducting online surveillance of peer-to-peer networks. However, TOR makes the IP address inaccessible, prompting the question of whether the use of TOR creates a reasonable expectation of privacy by itself. Eduardo R Mendoza, "Network Investigation Techniques: Government Hacking and the Need for Adjustment in the Third-Party Doctrine" (2017) 49:1 St Marys LJ 237 at 256.

[1458] West & Forcese, *supra* note 85 at 18. For an example of where a general warrant and a Part VI authorization were combined to allow for the covert monitoring of the suspect's computer activity, see *R v Merritt*, *supra* note 791. In this specific case, the malware used for this monitoring had been previously installed by law enforcement on a computer that was then gifted to the suspects under false pretenses, as part of a covert investigation.

cost associated with it, and the time it takes to carry out the hacking.[1459] Yet, it has been suggested as possibly the best solution to the "going dark" problem, absent compelled decryption powers.[1460]

Lawful hacking, however, raises unique privacy considerations and can be perceived as being more intrusive than compelled decryption for a few reasons, First, it can give law enforcement continuous access to everything that is typed or accessed by the device in real time, which comes closer to a wiretap than an alternative to the search of the device following its seizure. Second, a longer period of monitoring a device is more intrusive than a one-time access.[1461] Third, it can also implicate third parties and give law enforcement unprecedented access to highly private areas, for example when remotely accessing a device's webcam while the device is in the suspect's home.[1462] It has recently been announced that a Parliamentary committee will examine the use of lawful hacking software by the RCMP, following a request on this matter made by the Privacy Commissioner of Canada.[1463]

[1459] Ahlam, *supra* note 1452 at 796; Ohm, *supra* note 1451 at 322.

[1460] See Liguori, *supra* note 70; Alexa Wainscott, "A Golden Key to Pandora's Box: The Security Risks of Government-Mandated Backdoors to Encrypted Communications" (2017) 44:1 N Ky L Rev 57 at 75; Bellovin, Blaze & Landau, *supra* note 197 at 5; Dheri & Cobey, *supra* note 77 at 19.

[1461] Skorvanek et al, *supra* note 1084 at 1041–1042.

[1462] For example, in *Canadian Security Intelligence Service Act (Can) (Re)*, 2019 FC 141, [2019] 2 FCR 359 the Federal Court examined if the use of an "implant" by the Canadian Security Intelligence Service (CSIS) respected s. 8 of the Charter. An "implant" in this context is a type of device (software or hardware) that is used to intercept communications and to remotely access the content of devices. In other words, it is a type of lawful hacking mechanism. The Federal Court determined that while the use of this device can possibly affect the rights of innocent third parties, the safeguards put in place by the CSIS (namely the imposition of search protocols that seek to confirm that the "implant" is deployed on a device that either belongs to the target or is being used by the target) were sufficient to prevent a violation of s. 8 of the Charter.

[1463] La Presse Canadienne, "Logiciels espions : le commissaire à la vie privée veut des évaluations d'impact", (8 August 2022), online: *Radio-Canada* <https://ici.radio-canada.ca/nouvelle/1904010/logiciels-espion-impact-commission-vie-privee>; La Presse Canadienne, "L'usage de logiciels espions par la GRC sera examiné par un comité parlementaire", (26 July 2022), online: *Radio-Canada* <https://ici.radio-canada.ca/nouvelle/1901122/grc-logiciels-espions-comite-parlementaire-vie-privee>; Philippe Dufresne,

The complexity of lawful hacking techniques also raises the question of whether the issuing judge understands precisely what they are authorizing, due to the complex nature of this technology.[1464] It can additionally create trial fairness disputes, as the state is usually vehemently opposed to disclosing the source code used to conduct its hacking activities.[1465] Similarly, when law enforcement is exploiting a vulnerability to conduct its lawful hacking, the question of reporting the vulnerability to the vendor or to the public is unresolved.[1466] In turn, this means that the same vulnerability used by the government can also be exploited by criminals if it is not corrected by the vendor.[1467] Conversely, if disclosed to the vendor, this can also mean that the specific attack used in one case is no longer available to law enforcement in a later case.[1468] Further, lawful hacking techniques can be employed on devices that are located anywhere in the world, once again prompting jurisdictional debates.[1469] Perhaps the only way to properly address these concerns is also to create a specific provision regulating the use of lawful hacking techniques by the government for investigatory purposes, although this heavily specialized investigative technique is unlikely to become

---

"Appearance before the Standing Committee on Access to Information, Privacy and Ethics (ETHI) on the Study of Device Investigation Tools Used by the RCMP", (8 August 2022), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2022/parl_sub_220808/>.

[1464] Aucoin, *supra* note 147 at 1461–1462.

[1465] *Ibid* at 1464; Steven M Bellovin et al, "Seeking the Source: Criminal Defendants' Constitutional Right to Source Code" (2021) 17:1 Ohio St Tech L J 1. It might also run afoul of the branch of public interest privilege often referred to as "police investigation technique privilege," see *R v Amer*, 2017 ABQB 651; *R c Mirarchi*, 2015 QCCS 6629 [*Mirarchi II*].

[1466] Bellovin, Blaze & Landau, *supra* note 197 at 50–63; Manpearl, *supra* note 2 at 88; Jaffer & Rosenthal, *supra* note 101 at 314; Sharon Bradford Franklin, "The Need for Countries to Establish Robust and Transparent Vulnerabilities Equities Processes" (2019) 6:1 Fletcher Sec Rev 45.

[1467] Dheri & Cobey, *supra* note 77 at 18; Penney & Gibbs, *supra* note 3 at 214.

[1468] West & Forcese, *supra* note 85 at 20; Rupinder K Garcha, "Nits a No-Go: Disclosing Exploits and Technological Vulnerabilities in Criminal Cases" (2018) 93:4 NYU L Rev 822; Murphy, *supra* note 1111 at 251.

[1469] See Sections 8.3 and 10.3 *infra*.

routinely used by law enforcement.[1470] For this reason, Canada should follow in the footsteps of the UK and create a lawful hacking regime, rather than adopt the American position and leave this technique unregulated.

C) No Distinction Should be Made Between Devices or Encryption Methods

In order to create a coherent legal framework, no distinction should be made between devices or encryption methods because compelled decryption amounts to legal compulsion, regardless of the method used to lock the data or device (biometric, alphanumeric, or other)[1471] and regardless of the device itself (computer, cell phone, smart watch, etc.). Unlocking a device, regardless of the decryption method, implies the same "expression of exclusivity, ownership, and control"[1472] over the device or data. This is consistent with the fact that individuals use passwords and biometric authentication measures in the same way, that is, to make data inaccessible to anyone but themselves.[1473] A principled approach to privacy and other *Charter* protections also dictates this conclusion.[1474]

Further, if a different procedure is applicable depending on the locking mechanism, individuals are simply going to adopt the method that is better protected, thus bringing law enforcement back to square one. Instead, if we give the same protection to various encryption methods, it is more likely that the plaintext will be accessible to law enforcement in the long

[1470] Ohm, *supra* note 1451 at 332.
[1471] Goldman, *supra* note 211; Leamon, *supra* note 1239 at 599.
[1472] Reitinger, *supra* note 1239 at 64.
[1473] As put by Cohen & Park, *supra* note 3 at 170, "[a]mong the encryption options available, many users may make their choice based largely on convenience, little surmising their decisions' potential implications on their legal rights." See also Brejt, *supra* note 948 at 1181; Lemus, *supra* note 220 at 555.
[1474] Lemus, *supra* note 220 at 538; Larkin, *supra* note 999 at 270.

run. Protecting encryption regardless of the exact mechanism being used also furthers the idea that privacy is not about hiding a wrong.

One major consequence of distinguishing between encryption methods also rests in the fact that biometric authentication methods are generally deemed more secure than alphanumeric passcodes.[1475] They are also more convenient, considering that they remove the requirement of having to memorize an alphanumeric code.[1476] Distinguishing between both mechanisms, probably to the detriment of protecting biometric authentication methods, would create an unjustifiable gap between legal and technological protections.

Some authors have suggested that biometrics should not be protected against compulsion because their production is not testimonial and does not require the use of the suspect's mental abilities.[1477] However, this view has arisen in the American context, which is very different from the Canadian experience with self-incrimination, considering that the SCC has recognized that self-incrimination can apply to real evidence.[1478]

D) The Applicable Burden of Proof Should be the 'Reasonable Grounds to Believe' Standard

Due to the strength of the privacy and self-incrimination interests at stake and the intrusiveness of the investigative technique,[1479] a *reasonable grounds to believe* standard should be applied to a compelled decryption provision. The quantity of core biographical data

[1475] Herrera, *supra* note 212 at 786; Antonio Vayas, "Say Cheese: How the Fourth Amendment Fails to Protect Your Face" (2021) 51:5 Seton Hall L Rev 1639 at 1647; Phelps, *supra* note 1313 at 464; Sherman, *supra* note 217 at 666.
[1476] Redfern, *supra* note 215 at 603.
[1477] See inter alia Shweiki & Lee, *supra* note 1002; Lyon, *supra* note 1251 at 65; Kerr, *supra* note 3.
[1478] *Stillman*, *supra* note 353; *SAB*, *supra* note 430 at paras 34–35; *R v Collins*, *supra* note 31 at 284.
[1479] *Kang-Brown*, *supra* note 229 at para 13.

found on digital devices alongside Commissioner Therrien's comments on the legitimacy of the lower *reasonable grounds to suspect* standard used by Bill C-13,[1480] are also compelling arguments in favor of a stricter standard, especially when considering that the SCC in *Hunter* concluded that this standard would normally be required for a search or seizure to be deemed reasonable under s. 8 of the *Charter*.[1481]

Law enforcement should be required to demonstrate under this standard that (1) no other "encryption workaround" is reasonably applicable; (2) compelled decryption is in the best interest of the administration of justice, having regard to the severity of the alleged infraction and the importance of the evidence; (3) the sought-after data (or sought-after device) is protected by an encryption method for which the suspect possesses the key, defined as being either an alphanumeric key or biometric authentication method; and (4) the plaintext will provide evidence with respect to the commission of the offence(s) under investigation.

E) An Obligation to Unlock or Decrypt, in Exchange for Adequate Immunity

The increased risk of unreliable confessions that results from compelled decryption can be mitigated by granting suspects immunity for the act of decryption, which means the state would be unable to use the act of decryption to prove ownership or control over the data. By removing the inferences that can be drawn from the act of decryption, the risk of unreliable confessions is effectively removed in a correlative manner.[1482] Alternatively, this could be

[1480] Therrien, *supra* note 811.
[1481] *Hunter*, *supra* note 31 at 167–168.
[1482] *S (RJ)*, *supra* note 343 at paras 145–146; *White*, *supra* note 388 at para 62.

done by creating a presumption that bars the Crown from inducing evidence that the accused decrypted a device or data-set introduced into evidence.

If we accept the conclusion that we need to create a compelled decryption power in order to adequately balance the opposite interests at play, act of decryption immunity needs to be granted to the suspect coerced into decrypting. Because the rationale behind creating such compelled decryption powers is that the data will sometimes be impossible to obtain due to the strength of modern encryption, then the act of decryption should not facilitate the Crown's case to meet when it comes to establishing ownership and control over the device or the data. This immunity has the advantage of allowing the state to use the decrypted data to prosecute the accused, while protecting that individual from the testimonial aspect of compelled decryption.[1483]

The Canadian criminal justice system already uniquely relies on immunities to alleviate the impact of self-incrimination on individual rights, while still promoting the search for truth in criminal cases.[1484] For example, in *Re Application under s. 83.28 of the Criminal Code*, the SCC found that an obligation to testify at investigative hearings for the purposes of gathering information on terrorism offences did not violate the principle against self-incrimination because the adequate immunities (i.e., use and derivative use immunity) were put in place by the applicable legislation.[1485] Similarly, in *White*, the SCC concluded that drivers could be compelled to make statements under a provincial statute but that the statement could not be subsequently used to incriminate them during a criminal trial.[1486] The immunity created by

[1483] Terzian, *supra* note 1220 at 1134.
[1484] See Sections 4.2.7 and 4.2.8 *supra*.
[1485] *Application under s. 83.28 of the Criminal Code (Re)*, *supra* note 378 at para 72.
[1486] *White*, *supra* note 388.

the SCC effectively balanced society's interest in discovering the truth and the individuals' right against self-incrimination.[1487]

Providing suspects with act of production immunity will sufficiently protect against the self-incrimination aspects of the act of decryption. While use and derivative use immunity are usually the solution when compulsion risks compromising an individual's self-incrimination interests,[1488] immunity needs only to be correlative with the scope of the infringement on individual rights. In addition, derivative use immunity should only be granted when the use of the evidence is at risk of undermining the fairness of the trial,[1489] which would not be the case considering the strict conditions law enforcement would need to follow to obtain a compelled decryption order.[1490] As such, if we treat the act of production considerations separately from the encrypted material considerations, act of production immunity is sufficient to address the self-incrimination aspect of compelled decryption. Further, the prevalence and sophistication of encryption technology certainly justify the creation of such new rule, which the SCC expressly allowed in *White*.[1491]

In *Re Application under s. 83.28 of the Criminal Code*, the SCC found that the constitutional exemption (that "provides a form of complete immunity from testifying where proceedings are undertaken or predominately used to obtain evidence for the prosecution of the witness")[1492] was also respected because, although the provision allowed for compelled testimony, there was no evidence that its predominant purpose is to obtain information to

[1487] *Ibid* at para 71.
[1488] Penney & Gibbs, *supra* note 3 at 235.
[1489] *S (RJ)*, *supra* note 343 at 550.
[1490] See Section 7.3 *infra*.
[1491] *White*, *supra* note 388 at para 44.
[1492] *Application under s. 83.28 of the Criminal Code (Re)*, *supra* note 378 at para 71.

prosecute the witness.[1493] When it comes to compelled decryption, the act of decryption is used to gather evidence to prosecute the target, which at first glance would seem impossible under the constitutional exemption to self-incrimination. Nevertheless, the constitutional exemption can still be interpreted as allowing this investigative power when we focus on the underlying rationales behind the principle against self-incrimination and the hybrid nature of password compulsion. Act of production immunity, combined with adequate restrictions put in place under s. 8, will mitigate the impact on self-incrimination rights, while still allowing the state to fulfil its obligation to investigate and prosecute crime.

The Ontario Court of Justice in *Shergill* determined that nothing short of full derivative use immunity could justify the s. 7 violation brought forward by compelling the accused to unlock his cell phone.[1494] However, by reconciling ss. 7 and 8, this is not necessary. Full derivative use immunity, which would preclude the state from using the plaintext to prosecute the accused, is not required in this case for a few reasons. First, the creation of the data itself was not compelled, only its decryption.[1495] Second, the testimonial aspect of decryption only relates to the inferences of ownership and control of the data, not to the data itself. Considering law enforcement would have been able to obtain the plaintext if it was not for encryption, derivative use immunity is not required.[1496] Nonetheless, without act of decryption immunity, the section 7 violation identified *supra* remains.

When examining the applicable immunities, Parliament should also consider the possibility of restricting the use of the plaintext to the offences listed in the warrant. This would further

---

[1493] *Ibid* at para 72.
[1494] *R v Shergill*, *supra* note 230 at para 40.
[1495] Penney & Gibbs, *supra* note 3 at 240.
[1496] *Application under s. 83.28 of the Criminal Code (Re)*, *supra* note 378 at para 71.

limit the risk that this provision would be used to conduct 'fishing expeditions.' It would also address the general problem of the scope of digital searches.

F) Evidentiary Considerations Linked to the Use of Encryption and the Refusal to Decrypt Following a Legally Issued Order

The fact that suspects or accused individuals have encrypted their data or devices should not be used to draw negative inferences towards the encrypted contents, because individuals have valid reasons to want to protect their data in such way.[1497] As such, clear directives should be given to juries that the use of encryption should not generally be equated with a desire to hide evidence or unlawful material, absent strong circumstantial evidence that the encrypted material is indeed unlawful but inaccessible.[1498] This directive would at least partially address the faulted "nothing to hide" rhetoric.

However, if a person validly compelled to decrypt refuses to do so, some consequence should be attached to this refusal. To avoid punishing individuals who have genuinely forgotten their passwords, this punishment should be done by creating a new offence rather than by using the common law offence of contempt. This offence should include the necessity for the Crown to prove beyond a reasonable doubt that the individual knew the passcode or had access to it, rather than simply having failed to respect a court order. In creating the offence, Parliament would also have the opportunity to determine what sentence is appropriate to encourage

[1497] *R v Sonne*, 2012 ONSC 2126 at paras 18–19.

[1498] See for example, *R v CCM*, 2012 MBQB 141 at para 65, in which the Court concluded that the totality of the evidence supported the finding that child pornography pictures were placed by the accused in an inaccessible encrypted file. See also *R v Burke*, 2015 SKPC 173 at para 17.

individuals to comply with the order, rather than refuse to decrypt to avoid being accused of the main offence under investigation.

7.3.2 Considerations Under Section 1 of the Charter

In the event that the compelled decryption framework suggested above would be deemed to be contrary to ss. 7 or 8 of the *Charter*, it would need to be examined under s. 1, following the test established in *R v Oakes*.[1499] Under this test, a limitation placed on a *Charter* right will be deemed as reasonable and demonstrably justified in a free and democratic society if: (1) it serves an objective "of sufficient importance to warrant overriding a constitutionally protected right or freedom,"[1500] (2) that the means chosen are reasonable and demonstrably justified under a proportionality test.[1501] This proportionality test relies on three sub-factors:

> First, the measures adopted must be carefully designed to achieve the objective in question. They must not be arbitrary, unfair or based on irrational considerations. In short, they must be rationally connected to the objective. Second, the means, even if rationally connected to the objective in this first sense, should impair "as little as possible" the right or freedom in question: *R. v. Big M Drug Mart Ltd.*, *supra*, at p. 352. Third, there must be a proportionality between the effects of the measures which are responsible for limiting the *Charter* right or freedom, and the objective which has been identified as of "sufficient importance".[1502]

Hayes concluded that compelled decryption would always contravene s. 7 of the *Charter*. Accordingly, he examined whether s. 1 of the *Charter* could nonetheless save a compelled

---

[1499] *R v Oakes*, [1986] 1 SCR 103 [*Oakes*].
[1500] *R v Big M Drug Mart*, *supra* note 549 at 352, cited in *Oakes*, *ibid* at para 69.
[1501] *Oakes*, *ibid* at para 70.
[1502] *Ibid* (underlined in the original).

decryption provision. He suggested that the *Oakes* test could be satisfied in the context of compelled decryption in the following manner:

> The pressing and substantial objective of [a] proposed [compelled decryption] law would be to allow police to access devices which they are lawfully authorized to search to aid in criminal investigations. Requiring the accused to unlock their device and facilitate such a search provides the necessary rational connection between the law and this objective. Minimal impairment could be achieved by applying this law only to situations where a search has been judicially authorized via search warrant, not warrantless searches like in *Fearon.* The cost/benefit analysis comes down to a balancing of the *Charter* rights that would be infringed by this proposed law with the state's interest in effective law enforcement and public confidence in the administration of justice.[1503]

This thesis has submitted, quite contrary to Hayes' position, that compelled decryption would not be found to contravene ss. 7 or 8 of the *Charter*, if the compelled decryption framework submitted *supra* is respected. As such, the *Oakes* test would be inapplicable here. Nonetheless, it is conceded that if the abovementioned framework was found to violate s. 7 of the *Charter* specifically, it is unlikely that it could be saved under s. 1. Indeed, if s. 7 is infringed despite the stringent conditions suggested previously, it forces the realization that the principle against self-incrimination dictates that compelled decryption can never respect s. 7. The only possible exceptions to this would likely be in the case of exigent circumstances or for the investigation of offences relating to national security.[1504] Henceforth, the *Oakes* proportionality test would not be satisfied, even with the inclusion of strict requirements pertaining to the issuance of a

[1503] Hayes, *supra* note 339 at 11.

[1504] This would be coherent with the fact that the interception of private communications without a warrant has been deemed to be acceptable in such situations, even if the interception of privacy communications raises enhanced privacy expectations. See Section 5.3.3(B)(iv) *supra*.

compelled decryption authorization.[1505] This is also consistent with SCC's comments on the unlikelihood that a s. 7 violation could be justified under s. 1 of the *Charter*.[1506]

[1505] Due to the main claims made *supra*, a detailed application of the *Oakes* test is out of the scope of this thesis. The complexity of applying the *Oakes* test to a specific situation is evident from the SCC's jurisprudence on this subject. See for example *R v Brown*, 2022 CSC 18, which is the latest SCC decision examining this issue. Accordingly, this is a discussion better left to another time.

[1506] *Canada (Attorney General) v Bedford*, 2013 SCC 72, [2013] 3 SCR 1101 at para 129 [*Bedford*], referring to *Re BC Motor Vehicle Act*, [1985] 2 SCR 486 at 519.

CHAPTER 8 LAW ENFORCEMENT ACCESS TO ENCRYPTED DATA FROM SERVICE PROVIDERS

When the investigation of the San Bernardino shooting was stalled by the strength of the encryption on the suspect's iPhone, law enforcement tried to compel Apple to modify the software found on the device in order to facilitate the unlocking of the device using a brute-force attack, prompting a new nation-wide debate on the regulation of encryption.[1507] While ultimately the device was unlocked by a third party, making the issue moot, this case raises the important question of whether law enforcement should be able to compel third party service providers (TPDCs) into retaining decryption or unlocking capacities.

It appears that prior to 2014 Apple indeed agreed to unlock devices for various law enforcement agencies.[1508] However, in response to the Snowden revelations of 2013, the company decided to encrypt its devices in a manner which makes them impossible to unlock, short of hacking the device.[1509] In reaction to this decision, some have called for the regulation of the strength of encryption, while others have argued for exceptional access mechanisms to be implemented in devices and software.[1510] Essentially, the proponents of this second approach argue that the government should mandate TPDCs to include an access point—i.e.,

---

[1507] The iPhone in question was equipped with a data wipe feature that wipes all the data found on the device after 10 incorrect password attempts. Without this feature, the FBI would have been able to unlock the device in less than a day, due to the fact that the password was only 4 or 6 digits. See Babiarz, *supra* note 1354 at 364–365.

[1508] See for example *R v Millard and Smich*, 2016 ONSC 348 at para 10, in which Apple extracted all the data from the suspect's locked iPhone, following a Canadian issued assistance order. See also Potapchuk, *supra* note 138 at 1405; Ian J McCarthy, "iOS Fear the Government: Closing the Back Door on Governmental Access" (2017) 49:1 U Toledo L Rev 179 at 179.

[1509] Craig Timberg, "Apple will no longer unlock iPhones for police", (18 September 2014), online: *Police1* <https://www.police1.com/legal/articles/apple-will-no-longer-unlock-iphones-for-police-pJmeWqziSHVBN4AP/>.

[1510] See for example Corn, *supra* note 296.

a backdoor, a specific type of vulnerability implemented deliberately by the TPDC to retain unlocking or decryption capacity—into their software or devices. This type of exceptional access could then be used by the authorities to access the plaintext version of the data stored on a device, after obtaining the appropriate judicial authorization, without implicating the protection against self-incrimination.

The attempt to circumvent encryption applied to data at rest with the help of TPDCs is not limited to cases where a device manufacturer could be compelled into breaking its own protection measures. Indeed, cloud service providers can also be the subject of law enforcement requests to access data that belongs to a suspect but that is saved on the company's cloud platform. The architecture of cloud computing itself makes it possible for anyone with the correct credentials to access the data stored in the cloud,[1511] making this option a good "encryption workaround" when a suspect uses cloud computing.[1512] However, cloud service providers are also increasingly protecting their customers data in a manner that makes it impossible for them to decrypt.[1513]

This chapter will start by examining whether current court authorizations can be used to obtain data from a cloud service provider or to compel TPDCs to unlock devices. It will then investigate the question of whether the government should be able to compel TPDCs to manufacture their products in such way as to maintain decryption or unlocking capacities for

[1511] Colarusso, *supra* note 6 at 82.

[1512] Sacharoff, *supra* note 20 at 220–221.

[1513] Some cloud service providers guarantee to their customers that they will not access their data and effectively do not have the technological means to do so. See for example Mozy, "Privacy Statement", online: <https://mozy.com/about/legal/privacy>; SpiderOak, "Privacy Policy", online: *SpiderOak* <https://spideroak.com/privacy-policy/>. However, Apple keeps a copy of its customers iCloud encryption keys, in case they lose them. See Zittrain et al, *supra* note 296 at 11.

data at rest, whether stored locally on a device or delocalized on the cloud. Essentially, it will be argued that the regulation of encryption in such manner should not be considered as a solution to the encryption problem, as it would unduly affect data security at large. Finally, the jurisdictional issues prompted by the delocalization of data will be surveyed, although in a superficial way as this thesis focuses on Canadian domestic criminal law, not transnational or international law *per se*.

It should be noted that the current chapter examines only data at rest, not data in transit. The particular issue of the impact of encryption on data in transit will be examined separately in Chapter 10.

8.1 Compelling TPDC Collaboration Through Current Court Orders

As it currently stands, the *Criminal Code* contains two different types of authorizations that can be used to compel TPDCs to cooperate with the authorities in order to access the plaintext that is relevant to an investigation: assistance orders and production orders.

8.1.1 Assistance Orders (s. 487.02 of the Criminal Code*)*

First, when facing a locked device, the authorities can obtain an assistance order under s. 487.02 of the *Criminal Code* to compel the TPDC to unlock the device or to extract the data found within the device.[1514] It seems that in at least one instance, this order was used to force

[1514] *R v Millard and Smich*, *supra* note 1508 at para 10.

a TPDC to modify its software to make encrypted emails accessible to law enforcement.[1515] As summarized by Gill et al.:

> To facilitate FBI access, a British Columbia court issued an order which compelled Hushmail to develop and engineer an entirely new mechanism which would allow the company to extract a single user's decryption key from the decryption mechanism itself. Hushmail could do so because the mechanism in question was controlled by the company, and hosted and operated on Hushmail's own infrastructure. Hushmail was then obligated to obtain the targeted individual's key and use it to decrypt the target's emails through this newly-developed exploit.[1516]

The company reported having never contested a court order issued by the British Columbia Supreme Court.[1517] Accordingly, the validity of using a s. 487.02 assistance order to compel a TPDC to modify its encryption practices has not been tested before the courts.[1518] Similarly, it is unclear what would happen if a TPDC served with a similar assistance order did not have the technical capacity to respect the order, or refused to do so based on the possible impact of respecting the order on its commercial reputation. These questions are arguably better answered by Parliament than by the courts, which are not in a good position to make a fully informed decision about the regulation of encryption.[1519]

[1515] Ryan Singel, "Encrypted E-Mail Company Hushmail Spills to Feds", (11 July 2007), online: *Wired* <https://www.wired.com/2007/11/encrypted-e-mai/>, cited in Gill, Israel & Parsons, *supra* note 3 at 64. It seems from the Wired article that the emails were not intercepted while in transit, but rather accessed from the company's servers, once arrived at their destination. As such, the assistance order would have been accessory to a production order, not a wiretap authorization.

[1516] Gill, Israel & Parsons, *supra* note 3 at 64.

[1517] Singel, *supra* note 1515.

[1518] In the United States, a similar provision contained in the *All Writs Act* was interpreted by one court as applicable to compel a technology company to unlock a device, while another court reached the opposite conclusion. Babiarz, *supra* note 1354 at 364–367.

[1519] See Section 8.2 *infra.*

8.1.2 Production Orders (ss. 487.014 and following of the Criminal Code*)*

Second, when seeking data found on the cloud, law enforcement can use one of the many production orders found within the *Criminal Code*, depending on the exact nature of the sought-after data.[1520] Generally, if the data has been created by the suspect and is in cloud storage, a general production order under s. 487.014 of the *Criminal Code* would be required. In order for this provision to apply, we must consider that the TPDC has possession or control of the sought-after data, which in itself is not as clear as it may seem, especially when encryption is applied in such manner that the TPDC cannot access the data in a plaintext form. Indeed, can we really say that a TPDC is in control of the data if it is stored on its servers but unreadable? It would seem that in such a case, the TPDC can only be deemed to be in control of the encrypted data, not the plaintext version of that same data.[1521] In any case, and as put by Gill et al.:

> A production order does not require the service provider to design their technology in such a way that it facilitates law enforcement access to "useful" information. For example, if the information sought about a user is only available to a service provider is [sic] in encrypted form, a production order would not require the service provider

[1520] When seeking data found on a suspect's cloud, law enforcement officials have a few options. First, they can use a search warrant to seize the suspect's devices and then use these devices to access the cloud. Second, they can seek cooperation from the appropriate cloud service provider by using production orders. This option has been deemed to be better at protecting the data of innocent users. Third, law enforcement could obtain a search warrant and seize the cloud service provider's servers. However, this would be technically and logistically difficult, considering the size of the servers. It would also imply the collect of data belonging to innocent third parties. See Sarit K Mizrahi, "The Dangers of Sharing Cloud Storage: The Privacy Violations Suffered by Innocent Cloud Users during the Course of Criminal Investigations in Canada and the United States" (2017) 25 Tulane J Int'l & Comp L 303 at 321.

[1521] As stated by Halefom H Abraha, "Regulating law enforcement access to electronic evidence across borders: The United States approach" (2020) 29:3 Inf & Comm Tech L 324 at 333–334, "control" over data is subject to different interpretations. Following the most prevalent interpretation that stems from the Council of Europe's *Convention on Cybercrime*, a TPDC will be considered to have possession or control over the data if legally and technically the TPDC can access the data.

> to actively engineer a new mechanism to subvert its security measures in order to acquire that information in plaintext form.[1522]

Accordingly, when encryption is applied by the user directly, the TPDC will probably be unable to provide law enforcement with readable, decrypted data. However, if the encryption is applied by the TPDC, then it will likely be able to decrypt the data and to provide law enforcement with the data in its decrypted form.[1523]

When contemplating the use of a production order as an alternative to the seizure of the suspect's device, law enforcement needs to consider that the data saved on the cloud is not necessarily the same as the data found on a device,[1524] although some people use the cloud exclusively to back-up their data. As such, this "encryption workaround" will not automatically provide law enforcement with as much useful data as accessing the plaintext of the data found on a device might. It can nonetheless be very useful to obtain the data that a suspect has saved on the cloud, regardless of whether it is an exact replica of what suspects have saved locally on their devices.

Using the cloud as delocalized storage raises question about the nature of this data. In one sense, data that has arrived at its destination in the cloud is data at rest: only the location of the data changes. In another sense, because the cloud is a remote service, using it necessarily entails transferring data from a personal digital device to the cloud, giving it characteristics of data in transit for a short period of time. This can also be done in a dynamic manner, for example when editing a document on a cloud software platform, such as Microsoft OneDrive,

[1522] Gill, Israel & Parsons, *supra* note 3 at 62.
[1523] Mizrahi, *supra* note 1520 at 310–311.
[1524] Jaffer & Rosenthal, *supra* note 101 at 297.

which uses the "software as a service" model.[1525] Depending on the moment at which law enforcement is trying to access the data, different court authorizations might be required. In the case where law enforcement is trying to access the data once it has reached its destination, a production order would be sufficient, while a general warrant or Part VI authorization might be required in the other.[1526]

A production order could also theoretically be used to compel the production of a decryption key,[1527] if a TPDC has access to it. However, most producers of devices do not have access to the key used to unlock the device, whether alphanumeric or biometric, as these are saved locally on the device itself.[1528] The production orders found in the *Criminal Code* are consequently of limited use to law enforcement when it comes to gaining access to the sought-after plaintext, in the absence of a larger scheme imposing decryption abilities on TPDCs.

[1525] Software as a service (or SaaS) "is on-demand access to ready-to-use, cloud hosted application software." See IBM Cloud Education, "IaaS versus PaaS versus SaaS", (2 September 2021), online: *IBM* <https://www.ibm.com/cloud/learn/iaas-paas-saas>. When SaaS is used, the user does not need to previously download the software. Rather, the software is used remotely, using cloud services. As such, when a SaaS text-editing software is used, the user is in constant communication with the server where the software is hosted.

[1526] The issue with using a production order to intercept the data on its way to the cloud is that the cloud service provider is not in "possession or control" of the data at that exact time, hence the requirements found in s. 487.014(1) of the *Criminal Code* are not fully met. While this might seem like a trivial question due to the speed at which data can be transferred to the cloud, it is important to distinguish both because access at the end point and access in transit are not the technically the same. For example, consider the difference between accessing messages that have arrived at their destination, and messages that are intercepted in transit. See *Jones II*, *supra* note 249.

[1527] Gill, Israel & Parsons, *supra* note 3 at 63; Dheri & Cobey, *supra* note 77 at 27. However, West & Forcese, *supra* note 85 at 13 contend that is would only be possible if the key itself affords evidence of a criminal offence.

[1528] Babiarz, *supra* note 1354 at 353–354. However, some online service providers may have access to the key or passcode used by its customers, as a safeguard if the key or passcode was to be forgotten by the customer.

8.2 Legislation Concerning "Backdoors" and/or the Restriction and Regulation of Encryption

The idea to regulated encryption through some exceptional access scheme is not new. As seen previously in Chapter 2, the United States government proposed a key escrow scheme in the 1990s with the "Clipper Chip." The Chip would have allegedly allowed strong encryption to be employed on devices, while ensuring that the state could access data and communications in their decrypted form, by providing the government with a copy of each individual key.[1529] Although the program was eventually abandoned, mostly due to public outcry, the lessons from that era are very much applicable to the current iteration of the encryption-control debate.

8.2.1 Technical Arguments Against Exceptional Access Mechanisms

Exceptional access can be granted to law enforcement using two mechanisms: backdoors or key escrow. The first, as mentioned, is a vulnerability left in the device that would only be known to the government.[1530] The second relies on the mechanism behind symmetric and asymmetric key encryption[1531] to provide law enforcement with a copy of the key used to encrypt and decrypt data.[1532] While some exceptional access regimes exists in Canada when it comes to telecommunications,[1533] they do not cover encryption applied to data at rest, whether on devices themselves or on the cloud.[1534]

[1529] Gill, *supra* note 3 at 448.
[1530] Opderbeck, *supra* note 3 at 1663.
[1531] See Section 2.3.1 *supra*.
[1532] Opderbeck, *supra* note 3 at 1663–1667.
[1533] See Chapter 9 *infra*.
[1534] Penney & Gibbs, *supra* note 3 at 218.

Malware cannot operate without exploiting a vulnerability in the targeted device's security system.[1535] This means that in order to successfully use lawful hacking to circumvent encryption, as suggested in Chapter 7 and presented as a good solution to the "going dark" problem,[1536] a vulnerability must be present. For this reason, forcing corporations to include backdoors into their systems has been argued to be a better alternative.[1537] However, many authors have reached the conclusion that backdoors are inherently insecure and could be exploited by malicious actors.[1538] The regulation of encryption by limiting the length of available encryption keys has also been found to create security weaknesses.[1539] Dheri and Cobey summarize the security repercussions of backdoors as follows:

> Backdoors build vulnerabilities into technology everyone uses, including governments and law-abiding citizens. While criminals use encryption to conceal evidence from state agencies, the reverse dynamic is also true. Governments rely on encryption to secure valuable state information, and criminals and terrorists often use workarounds to try to defeat it. Backdoors cannot be installed to make criminal communications [or data] vulnerable without, at the same time, making government

[1535] Ohm, *supra* note 1451 at 312.
[1536] Liguori, *supra* note 70; Skorvanek et al, *supra* note 1084; Gonzalez, *supra* note 1438 at 28; Ahlam, *supra* note 1452 at 835; Chen, *supra* note 3 at 195.
[1537] Gill, *supra* note 3 at 452.
[1538] Swire & Ahmad, *supra* note 39 at 460; Dheri & Cobey, *supra* note 77 at 4; Gonzalez, *supra* note 1438 at 3; Kaye, *supra* note 112 at 4; Hurwitz, *supra* note 69 at 413; Wainscott, *supra* note 1460; Penney & Gibbs, *supra* note 3 at 219–220; Potapchuk, *supra* note 138 at 1418; Dustin Taylor Vandenberg, "Encryption Served Three Ways: Disruptiveness as the Key to Exceptional Access" (2017) 32 Berk Tech LJ 531 at 559; Paul McLaughlin, "Crypto Wars 2.0: Why Listening to Apple on Encryption Will Make America More Secure" (2016) 30:2 Temp Int'l & Comp LJ 353; McCarthy, *supra* note 1508 at 191; *The Encryption Debate in the European Union: 2021 Update*, by Maria Koomen (Washington, DC: Carnegie Endowment for International Peace, 2021) at 4; Aylward, *supra* note 655 at para 84; Chan & Aylward, *supra* note 298 at 15; Chen, *supra* note 3 at 194; Diab, *supra* note 3 at 270; Murphy, *supra* note 1111 at 260.
[1539] Gill, Israel & Parsons, *supra* note 3 at 43.

> and individual communications [or data] susceptible to criminal, terrorist, or foreign hacking.[1540]

In addition to being insecure, backdoors have also been deemed to be unnecessary when it comes to lawful hacking, as it is largely acknowledged that no code is perfect and that vulnerabilities will always be found in software.[1541] The European Agency for Network and Information Security (ENISA), alongside Europol, issued a statement calling for alternative investigative techniques to be found, in replacement of any technique that would negatively impact the strength of encryption.[1542]

In 2015, a group of experts, mostly comprised of computer scientists and engineers, examined the feasibility of regulating encryption by providing exceptional access to law enforcement and the government in general.[1543] Their conclusions are clear: exceptional access, whether by backdoors, key escrow (also sometimes called split-key approach[1544]), or other limitations put on encryption, would "put the security of Internet infrastructure at risk."[1545] Specifically when it comes to encryption applied to devices and data at rest, the imposition of a requirement upon TPDCs to maintain unlocking capacities is unlikely to be realistic from a technological perspective.[1546] Put simply, any exceptional access scheme would create

---

[1540] Dheri & Cobey, *supra* note 77 at 10.
[1541] Kerr & Schneier, *supra* note 22 at 1006.
[1542] ENISA & EUROPOL, "On lawful criminal investigation that respects 21st Century data protection", (20 May 2016), online: <https://www.europol.europa.eu/cms/sites/default/files/documents/on_lawful_criminal_investigation_respecting_21st_century...%20%281%29.pdf>.
[1543] Abelson et al, *supra* note 3.
[1544] Geoffrey S Corn, "Averting the Inherent Dangers of Going Dark: Why Congress Must Require a Locked Front Door to Encrypted Data" (2015) 72:3 Wash & Lee L Rev 1433 at 1445.
[1545] Abelson et al, *supra* note 3 at 9.
[1546] *Ibid* at 14–15. See also Hurwitz, *supra* note 69 at 414.

substantial security risks, in addition to high engineering costs and other types of collateral damage,[1547] including damage to a company's reputation.[1548] As put by Gill et al.:

> There is, in fact, an unwavering consensus within the technical community that any exceptional access system will undermine encryption security by dramatically increasing complexity and related opportunities for exploitation. […] While some members of the technical community have sought to identify exceptional access systems that are "as secure as possible" in early 2018, nothing has disturbed the long-standing consensus that backdoors and similar proposals fundamentally weaken the security of communications products and endanger users. This position is virtually as unanimous among computer scientists as the existence of climate change is among environment scientists.[1549]

The suggestion of implementing a backdoor on an *ad hoc* basis, i.e., creating a backdoor that could only be used against a specific device, in a specific investigation, has also been said to be impossible, as once code exists it can easily be replicated and cannot truly be destroyed.[1550] Apple's CEO Tim Cook has stated that any attempt to create a software to bypass its security feature would basically create a "master key," that could be used to unlock all its devices,[1551] making every device vulnerable.[1552]

[1547] Abelson et al, *supra* note 3 at 21; Lear, *supra* note 72 at 470–471.
[1548] Ahlam, *supra* note 1452 at 827–828; Lear, *supra* note 72 at 471.
[1549] Gill, Israel & Parsons, *supra* note 3 at 54.
[1550] Gregory Coutros, "The Implications of Creating an iPhone Backdoor" (2016) 6:2 Nat"l Sec L Brief 81 at 81.
[1551] As cited in McCarthy, *supra* note 1508 at 181.
[1552] Surprisingly, after being very vocal about the inherent insecurity of backdoors, Apple has announced in 2021 new features that are presented as "protections for children" but that have been criticized as essentially being a backdoor by another name. These new features are two-fold: first, Apple will scan every photo that gets uploaded into iCloud photos to see if they constitute child pornography, using a database of known child abuse material. Second, every iMessage sent or received on devices linked to a child account will be scanned for sexually explicit material, once the feature is activated by a parent. See India McKinney & Erica Portnoy, "Apple's Plan to 'Think Different' About Encryption Opens a Backdoor to Your Private Life", (5 August 2021), online: *Electronic Frontier Foundation* <https://www.eff.org/deeplinks/2021/08/apples-plan-think-different-about-encryption-

The question then becomes whether, as a society, we are willing to compromise the digital security of entire populations, not to mention that of their governments, in order to obtain evidence in very specific criminal cases where encryption is an impediment to law enforcement's power to investigate. It also raises the question of whether jurists are in a position to dictate what is technologically feasible when it comes to digital privacy and security, in addition to the overarching question of whether the government has the power "to compel a private corporation to build something for a government purpose."[1553]

8.2.2 Rights-Based Arguments Against Exceptional Access Mechanisms

Even if it is technically feasible to regulate encryption by compelling TPDCs to include backdoors in their products, as a minority of authors suggest,[1554] there are strong arguments against it from a rights-based perspective. If there is one thing that the Crypto Wars taught us, it is that society in general has a strong distaste for the regulation of encryption.[1555] As such, an attempt to impose key escrow schemes or to mandate TPDCs to maintain decryption capacity would likely be met by strong opposition, on the basis that it would infringe individual rights and liberties.

A caveat is required here. This thesis will focus exclusively on the potential infringement of s. 8 of the *Charter* that would stem from regulating encryption at the TPDC level. Other

---

opens-backdoor-your-private-life>. See also Nicholas A Weigel, "Apple's 'Communication Safety' Feature for Child Users: Implications for Law Enforcement's Ability to Compel iMessage Decryption" (2022) 25:2 Stan Tech L Rev 210; Koomen, *supra* note 1538.

[1553] Gonzalez, *supra* note 1438 at 9.

[1554] Manpearl, *supra* note 2; Corn, *supra* note 296 at 345; Corn, *supra* note 1544. In his 2015 article, Corn uses the terminology "front door," rather than "back door" to connote the idea that the "split key" method he suggests does not create a subterfuge method of accessing data. Regardless of the terminology employed, most authors and experts agree that these suggestions create vulnerabilities and diminish digital security.

[1555] Manpearl, *supra* note 2 at 69–70; Swire & Ahmad, *supra* note 39 at 435.

arguments could possibly be made under ss. 2(b) or 7 of the *Charter*.[1556] These are out of the scope of this thesis.

As was extensively explored earlier, individuals have a reasonable expectation of privacy towards their personal data and their communications, even when the data is shared with a third party or when the communication is conducted on an electronic communication platform provided by a TPDC.[1557] In addition, the deployment of encryption on a device or towards specific data amplifies that expectation of privacy, in part because of the unique interaction of the principle against self-incrimination with the protection against unreasonable search and seizure in the context of encryption.[1558] In accordance with the SCC's rejection of the risk analysis approach in *Duarte*,[1559] the risk that a backdoor could be used by the government to access decrypted data should not transform an otherwise reasonable high expectation of privacy into an unreasonable one.[1560] Accordingly, *the use* of a backdoor to circumvent

[1556] On a possible s. 2(b) violation, see Colangelo & Maurushat, *supra* note 110; Gonzalez, *supra* note 1438; Lear, *supra* note 72 at 469; Bonin, *supra* note 6 at 505; Babiarz, *supra* note 1354 at 369; Ryan, *supra* note 52 at 1201; Adrianna Oddo, "Being Forced to Code in the Technology Era as a Violation of the First Amendment Protection against Compelled Speech" (2018) 67:1 Cath U L Rev 211. The identification of a s. 7 violation would require an in-depth analysis of the SCC jurisprudence on this provision, which is too big an endeavour to undertake here, but at first glance parallels could possibly be drawn with the SCC's decision in *Bedford*. In *Bedford*, *supra* note 1506, the SCC determined that sex workers have the right under s. 7 of the Charter to institute certain safety measures to protect themselves from violence. This could be used as a starting point to examine whether individuals should have a right to defend themselves against unwanted intrusions into their data and personal devices by adopting strong encryption. In turn, these measures can prevent physical harm to an individual (for example, if a hacker used this information to attack the person or to break into their home) and psychological harm (for example, if intimate images were found by a hacker and then published online without the person's consent).

[1557] See Chapter 5.

[1558] See Section 7.2.2(A)(v) *supra*.

[1559] *Duarte*, *supra* note 607. Also restated in *Mills II*, *supra* note 264; *Marakah*, *supra* note 260.

[1560] Gonzalez, *supra* note 1438 at 26.

encryption and access personal electronic data would be a search under s. 8 of the *Charter* and would need to withstand s. 8 analysis in order to be constitutional.

Additionally, it is also submitted here that requiring TPDCs *to include* exceptional access mechanisms in their systems would constitute a search or seizure under s. 8 of the *Charter.* Not only do individuals have a reasonable expectation of privacy that the state will not be able to access their encrypted data and compel decryption absent prior judicial authorization, they also reasonably expect that the state will not weaken the protection that encryption affords to privacy by mandating TPDCs to include backdoors into their products. As mentioned previously, encryption is one of the last measures individuals can employ to ensure that third parties cannot invade their personal data at will, including cybercriminals. From a normative perspective, society would be unwilling to accept that the state can adopt legislation that so drastically augments the chance that a criminal offense will be committed against individuals.

Under s. 8 of the *Charter*, the use of investigative methods that impact a reasonable expectation of privacy must be authorized by law, the law itself must be reasonable and the search or seizure must also be carried out in a reasonable manner.[1561] Presently, no judicial authorization is applicable to force TPDCs to include backdoors into their products.[1562] Under the ancillary powers doctrine, law enforcement would not be able to compel TPDCs to include exceptional access mechanisms into their products, as it would constitute an "unjustifiable use of powers in the circumstances."[1563] As stated by J. Le Dain in *Dedman*, for this branch of the analysis to be respected "[t]he interference with liberty must be necessary for the

[1561] *R v Collins*, *supra* note 31 at 278.
[1562] Although some authorizations are applicable when it comes to accessing the data with the help of a TPDC, whether in encrypted form or in decrypted form. See Section 8.1 *supra*.
[1563] *Godoy*, *supra* note 620 at para 7.

carrying out of the particular police duty and it must be reasonable, having regard to the nature of the liberty interfered with and the importance of the public purpose served by the interference."[1564] This criterion would not be respected when it comes to an obligation imposed on all TPDCs, as this is not necessary in order for law enforcement to reach their investigative purposes. Further, it would not be reasonable in light of the impact it would have on society at large. Accordingly, the only way TPDCs could be compelled to include exceptional access mechanisms into their products would be by legislative action.

It is highly unlikely that government-mandated backdoors or other methods of exceptional access could be found to be reasonable under the second prong of the *Collins* test, in part because they would unduly put law-abiding users of devices or software at risk.[1565] There is a very important distinction to be made between the government using a pre-existing vulnerability that was discovered in software in a specific situation, as opposed to the government mandating its presence at large. Lawful hacking only impacts the targeted device's security, while mandated backdoors are a potential risk for any user of that type of device—which could be many users indeed.[1566]

Further, if the inclusion of a backdoor was mandated for every TPDC, individuals would have no way of knowing if their data was examined by law enforcement using the backdoor absent a prosecution.[1567] This would not mesh well with the preventative and protective nature of s. 8 of the *Charter*. It would also run the risk of being used by foreign governments that fail to

[1564] *Dedman*, *supra* note 453 at 35
[1565] Gliksberg, *supra* note 1330 at 789–790; Lear, *supra* note 72 at 469; Ryan, *supra* note 52 at 1190.
[1566] Ahlam, *supra* note 1452 at 796.
[1567] Taylor, *supra* note 3 at 232.

use 'front door access' (by using the mutual legal assistance (MLA) process, for example), which could enable human rights violations abroad.[1568]

Penney and Gibbs have argued that encryption in itself does not attract a reasonable expectation of privacy as once data is legally obtained "the law imposes no limits on [law enforcement's] efforts to make it intelligible."[1569] This is correct. As mentioned previously, encryption does not give individuals the right to expect that the state will not try to circumvent the encryption by using methods at its disposal, namely the "encryption workarounds" described *supra*. However, they use this argument to conclude that exceptional access mechanisms would not violate s. 8 of the *Charter*. To reach this conclusion, they use the analogy that individuals can lock their documents into a safe to keep them private but that the police are entitled to try to open the safe when equipped with a warrant.[1570] It is submitted here that exceptional access requirements are of a different nature, which cannot be analogized with trying to open a safe. It would be more akin to forcing safe makers to include a trap door in the back of every safe, to ensure that law enforcement is allowed to access its contents. This is simply untenable and unprecedented, when it comes to s. 8 of the *Charter*.

8.2.3 Policy-Based Arguments Against Exceptional Access Mechanisms

Further, and regardless of the constitutionality of any type of regulation put on encryption, there is a strong argument to be made about the efficiency of such measures, in light of the fact that criminals (and law-abiding citizens who are especially worried about their privacy) would most likely find ways to create and use alternative software or hardware that would not

[1568] Gill, Israel & Parsons, *supra* note 3 at 57.
[1569] Penney & Gibbs, *supra* note 3 at 222.
[1570] *Ibid*.

comply with any type of regulation imposed by the state.[1571] Indeed, "those users most concerned with the security of their documents, including those who believe they have incriminating information to hide, likely would continue to use encrypting devices with the highest possible security."[1572] This is made possible by the internet itself, which will always give a platform for those who wish to acquire strong encryption software and devices,[1573] *inter alia* on the dark web. This is also why the regulation of encryption via export control policies is unlikely to function,[1574] alongside its chilling effect on innovation and commercial competitivity.[1575]

Similarly, users could also simply refrain from updating their devices, in order to continue to benefit from software that does not contain a backdoor.[1576] In turn, this could expose them to other risks, but keep them immune from the government using the backdoor to obtain their data in a decrypted form. Once again, this puts consumers in the position of having to decide between securing their devices from the state or from hackers, which is untenable.

Instead of trying to weaken encryption as a solution to the "going dark" problem, from a policy point of view the state should encourage strong encryption and consider other options to circumvent encryption, such as the "encryption workarounds," lawful hacking, and in last

---

[1571] *Ibid* at 220.

[1572] Bonin, *supra* note 6 at 504. Manpearl, *supra* note 2 at 82 suggests that only sophisticated criminals would seek out other ways to encrypt their communications or devices if lawful access was imposed in a country. This argument is unconvincing for a few reasons. First, it does not take into account that encryption is increasingly sought-after by consumers. Second, it creates an arbitrary level of protection according to individual knowledge and computer proficiency.

[1573] Amnesty International, *supra* note 113 at 25; Hill-Smith, *supra* note 150 at 189.

[1574] Titi Nguyen, "Computer Security and the Law: Regulating the Export of Encryption" (2001) 1 L & Soc'y Rev UCSB 49 at 53.

[1575] Gill, Israel & Parsons, *supra* note 3 at 46–47.

[1576] Babiarz, *supra* note 1354 at 367.

resort the suggested compelled decryption framework presented in Chapter 7.[1577] These have the advantage of allowing law-abiding citizens and society in general to continue to benefit from the numerous advantages of encryption.[1578] The state could also compel assistance from TPDCs, using the existing provisions detailed in section 8.1, when the relevant TPDC already has access to the target's encryption key or to the sought-after data in plaintext. This is similar to what is done under *TOLA*, as the Australian government stated that the applicable provisions could not be used to impose backdoors.[1579] As seen in Chapter 6, *TOLA* explicitly prohibits a systematic weakening of encryption, either by imposing a specific key-length or by creating a key-escrow scheme.[1580] This approach is to be favored as it ensures that strong encryption remains available.[1581] Using pre-existing vulnerabilities to lawfully hack targets also has the positive effect of encouraging TPDCs to create more secure systems, in order to respond to customers' security expectations.[1582]

Actually, if Parliament decided to impose mandatory backdoors to TPDCs, the compelled decryption framework suggested in Chapter 7 would lose all its relevance, making it unjustifiable under s. 7 of the *Charter*, as it would not be necessary to adequately balance the

[1577] Some additional investigative techniques might be useful in specific types of cases. For example, specific techniques might yield interesting results when it comes to online child pornography. See Anthony G Volini & Farzana Ahmed, "Strategies to Deter Child Pornography in the Absence of a Mandatory Encryption Back Door: Tipster Programs, a Licensed Researched System, Compelled Password Production, & Private Surveillance" (2022) 32:1 DePaul J Art Tech & Intell Prop L 1.
[1578] See Chapter 2 and Dheri & Cobey, *supra* note 77 at 6–7, 11; Amnesty International, *supra* note 113 at 31.
[1579] Ahlam, *supra* note 1452 at 805.
[1580] Earls Davis, *supra* note 1139 at 5, 13.
[1581] It should be noted at this point that *TOLA* has been heavily criticized, including on the basis that it negatively impacts encryption, even if the act itself claims to encourage strong encryption. See *inter alia* Melanie Hutchinson, "Unintended Consequences and Australia's Assistance and Access Act 2018 - Is Australia Creating a Technology Based Human Rights Problem?" (2019) 12:47 Int'l In-House Counsel J 1; Joseph Cannataci, *Mandate of the Special Rapporteur on the right to privacy* (2018), online: *Office of the High Commissioner for Human Rights* <https://www.ohchr.org/sites/default/files/O_LAUS_6.2018.pdf>.
[1582] Ahlam, *supra* note 1452 at 843.

opposed interests of law enforcement and of citizens. Further, the promotion of strong encryption is better aligned with Canadian privacy laws, which already impose encryption requirements on corporations,[1583] in furtherance of the OECD *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*.[1584] It would seem contradictory to encourage strong encryption in one specific sphere of the law, while undermining it in another.[1585]

As presented in Chapter 3, encryption is beneficial for the state, as well as for individuals, as a method of promoting digital security, in a world where we rely increasingly on the internet and on digital devices. Consequently, any attempt to limit encryption at the source would not only negatively impact individuals' interest in digital security, but also the state's interest in national security. Encouraging strong encryption protects national security, rather than harming it in any way.[1586] Canada has historically been in favor of strong encryption[1587] and should remain committed to protecting its availability. For these reasons, any solution to the "going dark" problem that negatively impacts encryption—such as backdoors, key-length limitations, and key escrow schemes—should be dismissed by Parliament, effectively ending this debate in the same way the Crypto-Wars ended in the United States in the 1990s.

[1583] See principle 7 of *PIPEDA*, *supra* note 1018.

[1584] Organization for Economic Co-operation and Development, "Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data", online: *OECD* <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188>.

[1585] Wainscott, *supra* note 1460 at 60.

[1586] Lear, *supra* note 72 at 465–468; Taylor, *supra* note 3 at 245.

[1587] Parsons, *supra* note 56 at 2.

8.3 THE IMPACTS OF THE DELOCALIZATION OF DATA ON CRIMINAL INVESTIGATIONS

An intense and narrow focus on data location made sense when data could be transported between countries only by physically carrying storage media across borders. With the inception of the Internet and the ease of remote access to data, the concept of "location" is increasingly meaningless as well as irrelevant to data protection.[1588]

The jurisdictional challenges brought forward by internet-based technologies have been discussed for many years now. The "data is different"[1589] rhetoric has certainly been used by many authors, in different forms, ever since the mid-1990s, a time where this question mostly related to jurisdiction over crimes committed online, rather than investigative jurisdiction.[1590] Jennifer Daskal states that four characteristics of data make it different than any other evidence: its unique mobility, divisibility, location independence, and potential for third-party control.[1591] Famously, in 1996, John Perry Barlow wrote *A Declaration of the Independence of Cyberspace*, advocating for a self-governed internet that would be out of reach of traditional territorial jurisdiction.[1592] While his ideas never materialized,[1593] they definitely prompted a

[1588] W Kuan Hon & Christopher Millard, "Data Export in Cloud Computing - How Can Personal Data Be Transferred Outside the EEA: The Cloud of Unknowing, Part 4" (2012) 9:1 SCRIPTed 25 at 25. See also Paul Schiff Berman, "Legal Jurisdiction and the Deterritorialization of Data" (2018) 71 Vand L Rev 11 at 12, 14; Jennifer Daskal, "Borders and Bits" (2018) 71:1 Vand L Rev 179 at 188 to the same effect.

[1589] Schiff Berman, *supra* note 1588 at 13–14, referring to David R Johnson & David Post, "Law and Borders: The Rise of Law in Cyberspace" (1996) 48:5 Stan L Rev 1367, as being the first authors to make the "data is different" argument in relation with jurisdiction, sovereignty, and legitimacy issues caused by the internet.

[1590] For a timeline of how internet jurisdiction has been perceived throughout the years, see Schiff Berman, *supra* note 1588 at 13–20.

[1591] Daskal, *supra* note 1588 at 222–226.

[1592] John Perry Barlow, "A Declaration of the Independence of Cyberspace", (8 February 1996), online: *Electronic Frontier Foundation* <https://www.eff.org/cyberspace-independence>.

[1593] As put by Currie, *supra* note 35 at 12: "states do treat the Internet and the overall international communications infrastructure as a territorially bounded place." See also Bert-Jaap Koops & Susan W Brenner, eds, *Cybercrime and jurisdiction: a global survey*, Information technology & law series 11 (The Hague: West Nyack, NY: TMC Asser; Cambridge University Press, 2006) at 6; Daskal, *supra* note 1588 at 221.

world-wide reflection on the applicability of traditional jurisdictional rules to the new paradigms posed by the internet.

Since then, the issues related to the unique nature of jurisdiction over the internet might have become even more prevalent, due to the delocalization of data caused by cloud computing and the ever-increasing number of internet users.[1594] Digital device users are increasingly using cloud computing services, as an alternative to backing up their data locally on their devices, which means data that is relevant to an investigation is likely to be located on a third-party server, rather than on locally on a suspect's computer. Further, nowadays TPDCs will often have servers located all across the globe[1595] and will even sometimes be unable to locate specific data with exactitude.[1596] When TPDCs are compelled to hand over data under their control with a production order, or to remotely decrypt services with an assistance order, the

[1594] As put by Secil Bilgic, "Something Old, Something New, and Something Moot: The Privacy Crisis Under the CLOUD Act" (2018) 32:1 Harv JL & Tech 321 at 322: "[t]he emergence of cloud computing has exacerbated [the] frustration [caused by prolonged cross-border data access]."

[1595] For example, Google has cloud servers used for storage all over the world, including in Montreal, São Paulo, Zurich, London, Mumbai, Osaka and Sydney. Google, "Global Locations - Regions & Zones", online: *Google Cloud* <https://cloud.google.com/about/locations>.

[1596] In *British Columbia (Attorney General) v Brecknell*, 2018 BCCA 5 [*Brecknell*] the American company Craigslist was unable to tell the Court exactly where the relevant data was located. See also Raffaele Zallone, "Here, There and Everywhere: Mobility Data in the EU (Help Needed: Where is Privacy?)" (2013) 30:1 St Clara High Tech LJ 57 at 65. This is in part due to the fact that data stored in the Cloud is moved around from one server to another by ISPs and TPDCs, depending on the workload of each server. See Rebecca Eubank, "Hazy Jurisdiction: Challenges of Applying the Stored Communications Act to Information Stored in the Cloud" (2016) 7:2 Geo Mason J Int'l Com L 161. This practice of moving customer data is done "to minimize the use of storage centers at peak times, avoid down servers or power outages, and perform server maintenance without disrupting user access." See Jennifer Daskal, "The Un-Territoriality of Data" (2015) 125:2 Yale LJ 326 at 373; Mizrahi, *supra* note 1520 at 312–313. However, some "digital artifacts" left on a user's devices will usually make it possible to identify if that user has used the services of a specific cloud service provider.

location of the data can become problematic, as states do not have jurisdiction to conduct investigations on foreign soil.[1597]

These jurisdictional considerations are not limited to the "going dark" debate; rather they are linked to all electronic searches. However, some have said that "the greatest impediment to exceptional access may be the complexities of legal jurisdiction."[1598] This is in part due to the fact that any exceptional access mechanism imposed by a country has the potential of being used by any other countries, either through the MLA process or otherwise. This is especially worrisome when mandatory exceptional access is imposed by countries who "lack the comparatively robust procedural rights, legal, and political accountability mechanisms, and human rights protections by which countries such as Canada must abide."[1599] The limits of the applicability of an exceptional access mechanism are also unclear. For example, would a software developer based in country A need to respect an exceptional access requirement imposed by country B, if the software is being sold in country B?[1600]

Further, if lawful hacking is indeed accepted as an alternative to compelled decryption and exceptional access, the jurisdictional ramifications are also front and center, as law enforcement could be remotely accessing devices found in another country, without even knowing it. While there is no "absolute prohibition on cross-border cyberoperations [such as

[1597] As stated by Robert J Currie & Joseph Rikhof, *International & transnational criminal law*, third edition ed, Essentials of Canadian law (Toronto, ON: Irwin Law, 2020) at 57, 98, "enforcement jurisdiction," which includes "investigative jurisdiction" can only be exercised on the territory of the state, absent consent from the other state where it wishes to conduct its investigation. The applicability of this principle in the context of electronic data is, however, contested. See discussion in Section 8.3.1 *infra.*
[1598] Abelson et al, *supra* note 3 at 3.
[1599] Gill, Israel & Parsons, *supra* note 3 at 56.
[1600] Abelson et al, *supra* note 3 at 3.

'lawful hacking'] as a matter of international law,"[1601] the scope of a specific lawful hacking event might violate another state's sovereignty, in a climate where international norms on this matter are unclear.[1602] This could also be problematic in light of s. 487.01(6) of the *Criminal Code* which requires that a general warrant authorized under this section be executed within Canada, as well as under Part VI which also contains provisions regarding the location of the intercept.[1603]

This section will explore these considerations, ranging from the MLA process to the American *Clarifying Lawful Overseas Use of Data Act* (*CLOUD Act*)[1604] and related developments. It will examine Canadian decisions on the subject of access to data stored abroad and will consider whether data localization laws (i.e., laws that force companies to store data in the country of the user)[1605] should be implemented in Canada.

8.3.1 Accessing Data Stored Abroad

Without going into all the specific about the MLA process and the *Mutual Legal Assistance in Criminal Matters Act* (the *MLA Act*),[1606] it is useful to restate that traditionally states are unable to investigate crimes that have transnational aspects without requesting the help from the other implicated countries, either through the MLA process[1607] or with informal cooperation. For example, law enforcement officials from Montreal cannot show up at

[1601] Ahmed Ghappour, "Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web" (2017) 69:4 Stan L Rev 2075 at 1085.
[1602] *Ibid*.
[1603] See Section 10.3 *infra*.
[1604] United States, 115th Congress, *Clarifying Lawful Overseas Use of Data (CLOUD) Act*, HR 4943, 2018.
[1605] Bilgic, *supra* note 1594.
[1606] *Mutual Legal Assistance in Criminal Matters Act*, *supra* note 773.
[1607] For more details, see Currie & Rikhof, *supra* note 1597 c 9.

Apple's doorstep in California with a Canadian warrant allowing them to search the premises for documents that relate to a crime, even if this crime falls within the jurisdiction of Canadian courts. This is because under international law, states are prohibited from enforcing their own laws (including by way of law enforcement investigation) on the territory of other states.[1608] However, the dematerialization of evidence that occurred due to the advent and proliferation of internet-based technologies has had profound impacts on this general statement. It seems that Canadians law enforcement officials are now virtually knocking on TPDCs doors to request data pertaining to an investigation, using Canadian court orders, while being in Canada, regardless of the TPDC's location.

This issue has been addressed recently by different Canadian courts. In *Brecknell*, law enforcement officials were seeking data held by the American company *Craigslist*, on servers that could have been anywhere in the world, as no evidence relating to the specific location of the sought-after data was produced.[1609] To gain access to this data, the authorities applied for a general production order (s. 487.014 of the *Criminal Code*) from the courts in British Columbia, effectively trying to avoid going through the time-consuming MLA process. *Craigslist*, as with many other websites that offer their services in Canada, does not have a physical office in Canada, only a "virtual presence," but was nonetheless willing to respect a Canadian production order served to them via email.[1610] The lower courts nevertheless refused to issue the order, on the basis that they lacked jurisdiction to do so, prompting the Attorney General to appeal.[1611]

[1608] Currie & Rikhof, *supra* note 1597; *R v Hape*, 2007 SCC 26, [2007] 2 SCR 292.
[1609] *Brecknell*, *supra* note 1596 at para 14.
[1610] *Ibid* at para 13.
[1611] *Ibid* at paras 2–5.

After examining the relevant concepts emanating from *R v Hape*[1612] and from *Google Inc. v. Equustek Solutions Inc.*,[1613] the Court of Appeal of British Columbia determined that s. 487.014 of the *Criminal Code*, correctly interpreted, is applicable to anyone, corporation or physical person, that is within the jurisdiction of the issuing judge, regardless of the location of the sought-after documents or data.[1614] As such, when an entity has a physical presence in Canada, the location of the sought-after data seems irrelevant, as long as the company is able to access it from its Canadian offices.[1615] Justice Harris, writing for the Court, then went on to address the applicability of this conclusion when an entity is located outside of Canada, with only a "virtual presence" within the country. Based on the idea that "in the Internet era it is formalistic and artificial to draw a distinction between physical and virtual presence,"[1616] he concluded that the provision was indeed applicable to compel an entity with a "virtual presence" to respond to a Canadian production order.[1617] The "virtual presence" theory has since been followed or found correct by at least three other courts, in different provinces.[1618]

This decision was however not unanimously well-received by commentators or by other courts. Most notably, the Provincial Court of Newfoundland and Labrador (NLPC) strongly

---

[1612] *R v Hape*, *supra* note 1608.

[1613] *Google Inc v Equustek Solutions Inc*, 2017 SCC 34, [2017] 1 SCR 824. In this decision, the SCC concluded that an injunction with a global reach could be issued against Google because of the borderless nature of the internet.

[1614] *Brecknell*, *supra* note 1596 at para 39.

[1615] See *Application for production order (Re)*, 2020 NSPC 55 at para 24. This conclusion however runs contrary to what was decided in the United States following the Microsoft Ireland case. See *infra*.

[1616] *Brecknell*, *supra* note 1596 at para 40.

[1617] *Ibid* at para 60.

[1618] *Re Application for a Production Order, s. 487.014 of the Criminal Code*, 2019 ONCJ 775; *R v Love*, 2022 ABCA 269; *SPVM c JPM*, unreported decision [500-36-009870-216, 500-26-123252-219] (QCCS). Further, according to Daskal, *supra* note 1588 at 192–193, Belgium has adopted a similar approach to jurisdiction by concluding that its courts have jurisdiction over TPDCs offering their services to Belgians, even if the TPDC does not have a physical presence within the country.

disagreed with the *ratio decidendi* emanating from *Brecknell*, in a case where the sought-after data was held by *Facebook*, presumably on servers located in the United States.[1619] The NLPC, also analyzing the SCC's decision in *Hape*, concluded that in the absence of clear explicit language emanating from Parliament, the provision could not be interpreted has having extraterritorial reach, even though the internet does indeed create some difficulties when it comes to criminal investigations.[1620] Following this point of view, the MLA process would still need to be used by the authorities in order to obtain data from a company located abroad, regardless of whether we can consider that this company has a "virtual presence" in Canada. The sentiments worded by the NLPC found echo with commentators.[1621]

The problems caused by delocalized data are not unique to production orders. As seen in Chapter 5, s. 487(2.1) of the *Criminal Code* has been interpreted as allowing law enforcement to access a suspect's cloud with a search warrant, if this cloud is accessible from a seized device.[1622] Consequentially, this provision can also give law enforcement officials access to data that could be stored abroad, even in the absence of clear language that would indicate that this provision has a extraterritorial reach.[1623] While this may seem innocuous in a scenario

---

[1619] *In the matter of an application to obtain a production order pursuant to section 487.014 of the Criminal Code of Canada*, 2018 NLPC 2369.

[1620] *Ibid* at paras 26–27. See also David T Fraser, "Case Comment: *British Columbia (Attorney General) v. Brecknell*" (2020) 18:1 CJLT 135 at 136–141, on the absence of extraterritorial jurisdiction in the absence of explicit laws to that effect.

[1621] Currie & Rikhof, *supra* note 1597 at 519–520; Fraser, *supra* note 1620.

[1622] See for example *R v Stack*, *supra* note 780. See also Mizrahi, *supra* note 1520 at 346 and Ellyson, *supra* note 781 at 23 for a critique of this interpretation of s. 487(2.1) of the *Criminal Code*, in light of the fact that the provision was adopted when cloud computing was nowhere as prevalent as today.

[1623] Currie & Rikhof, *supra* note 1597 at 517; Andrew Matheson & John W Boscariol, "UK SFO unable to compel US company to produce documents held outside the UK", (20 April 2021), online: *McCarthy Tétrault* <https://www.mccarthy.ca/en/insights/articles/uk-sfo-unable-compel-us-company-produce-documents-held-outside-uk>; Fraser, *supra* note 1620; Christopher Naudie & John Cotter, "Enquêtes transfrontalières : la Cour d'appel de la Colombie-Britannique affirme son vaste pouvoir de lancer un processus judiciaire contre des sociétés étrangères", (18 December 2018), online: *Osler*

where the specific cloud platform is not encrypted and law enforcement is able to easily access the relevant data from the seized device,[1624] it could become problematic if the cloud platform is encrypted in such manner that the foreign TPDC's help is required to access the data in plaintext. In that specific case, it seems doubtful that a Canadian assistance order could be served directly onto a TPDC in order to compel assistance to circumvent encryption measures, under the "virtual presence" theory that originates in *Brecknell*. Thus, the issues regarding the transborder production of data by a TPDC are closely related to the encryption problem, especially in light of the fact that certain countries will have backdoor or decryption legislation and others will not, creating a confusing landscape of obligations for TPDCs and unclear privacy protection regimes for consumers.[1625]

Strictly from a logistics and policy perspective, the "virtual presence" concept is quite appealing. The MLA process can be quite burdensome, with its long delays[1626] and centralized processes. This can be especially problematic in light of the SCC decision *R v Jordan*, which prescribes rather strict delays in order for the right to be tried within reasonable time under s.

<https://www.osler.com/fr/ressources/transfrontaliers/2018/enquetes-transfrontalieres-la-cour-d-appel-de-la-colombie-britannique-affirme-son-vaste-pouvoir-de>.

[1624] In that case, the foreign country would most likely be unaware that law enforcement officials in Canada accessed a Cloud that falls within its jurisdiction. However, it is widely accepted that this type of practice does indeed constitute an unauthorized exercise of extraterritorial enforcement jurisdiction. See Currie, *supra* note 35 at 17. It is thus quite surprising that this provision has been interpreted this way, with virtually no discussion as to its potential extraterritorial reach.

[1625] It should be restated at this point that Australia's *TOLA* is made applicable to any TPDC offering its services within the country. See Chapter 6 and Jennifer Daskal, "Privacy and Security Across Borders" (2019) 128 Yale LJ Forum 1029 at 1044. It is further made accessible to international partners, via the MLA process. See McGarrity & Hardy, *supra* note 1140 at 176; Earls Davis, *supra* note 1139 at 4. Accordingly, this could create very confusing situations for TPDCs, if a foreign country tried to use these provisions to circumvent its own rules on decryption.

[1626] Jennifer Daskal cites another author who stated that the average delay to respond to MLAT requests in the US is 10 months. See Jennifer Daskal, "Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0" (2018) 71 Stanf L Rev Online 9 at 13. See also Joe Barton, "Reforming the Mutual Legal Assistance Treaty Framework to Protect the Future of the Internet" (2018) 79 Ohio St LJ Furthermore 91 at 93.

11(b) of the *Charter* to be respected.[1627] Investigations all over the worlds have been abandoned because of the delays linked to the MLA process.[1628] *A contrario*, accessing data directly through a TPDC would streamline the data-collection process and liberate Justice Canada's International Assistance Group (IAG)[1629] from many MLA requests, allowing for a better allocation of resources when it is still necessary to use a MLAT.[1630]

The delocalized nature of cloud computing and of the internet generally is also a strong argument in favour of this approach. Focusing on the localization of the servers hosting the data or the location of the TPDC does not reflect that cloud computing (when used as an off-site data storage solution) is simply a different method of storing personal data that would otherwise be found on a person's devices. The fact that the location of the sought-after data is not always known or easily determinable can also make it virtually impossible to obtain a MLA order, as the authorities will not always know to which country it needs to address its request.[1631] Jennifer Daskal also mentions that Microsoft has been said to design its system in a way where only its US-based offices are able to access data stored on its cloud regardless

[1627] *Jordan*, *supra* note 654.

[1628] Barton, *supra* note 1626 at 93 referring to *Transborder access to data and jurisdiction: Options for further action by the T-CY*, by Ad-hoc Subgroup on Transborder Access and Jurisdiction (Council of Europe - Cybercrime Convention Committee (T-CY), 2014) at 12.

[1629] Which is the designated central authority in charge of responding the MLA requests made under the *MLA Act*. See Currie & Rikhof, *supra* note 1597 at 574.

[1630] Barton, *supra* note 1626 at 98.

[1631] Abraha, *supra* note 1521 at 327; Bilgic, *supra* note 1594 at 329–330. Problematically, data can also be fractured onto different servers, located in different countries. It can also be moved around without human interaction. See Schiff Berman, *supra* note 1588 at 23; Shelli Gimelstein, "A Location-Based Test for Jurisdiction over Data: The Consequences for Global Online Privacy" (2018) 2018:1 U Ill JL Tech & Pol'y 1 at 12.

of the location of the server, which would mean that no country would have jurisdiction to access it if indeed the MLA system must be used.[1632]

However, the "virtual presence" theory indeed sits uneasily with widely recognized international law rules on comity and territorial jurisdiction,[1633] *inter alia* because it removes the possibility for the foreign government to control "access to their own citizens' or residents' data."[1634] The fact that the United States enacted the *CLOUD Act*[1635] in response to the *Microsoft Ireland* case[1636] is quite telling of the general consensus that the production of data located abroad will indeed implicate an extraterritorial use of a state's enforcement jurisdiction.[1637] The *CLOUD Act*'s main concern was to give American law enforcement agencies the power to compel the production of data from American TPDCs, regardless of the location of the data.[1638] Importantly, the *CLOUD Act* is applicable to corporations located outside of the United States, if it has "sufficient contact" with the US, such as a service

---

[1632] Daskal, *supra* note 1588 at 190. See also Gimelstein, *supra* note 1631 at 13.

[1633] Fraser, *supra* note 1620.

[1634] Daskal, *supra* note 1588 at 228.

[1635] As put by Bilgic, *supra* note 1594 at 333–334,

> "[t]he CLOUD Act introduces two novelties to cross-border data access. First, it carves out an exception for 'qualifying foreign governments,' allowing them to bypass the MLAT process. Qualifying foreign governments are those that have an executive agreement with the United States and have enacted laws that provide 'substantive and procedural opportunities' specified in the CLOUD Act to electronic communication service providers and remote computer providers. [...] Second, the CLOUD Act resolves the central question in the Microsoft Ireland case by creating s. 2713 of the [Stored Communications Act]."

This provision thus allows for the production of data located outside of the United States, if it is accessed from the United States.

[1636] In the *Microsoft Ireland* case, the matter in dispute was whether an American court order could be used to compel an American service provider to hand over to the authorities data found on a server in Ireland, that could nonetheless be easily retrieved from American soil. See Currie, *supra* note 35 at 3–4. See also Daskal, *supra* note 1626.

[1637] It should be restated at this point that "[t]he ban on extraterritorial enforcement jurisdiction is fairly straightforward and tends to be viewed restrictively and enforced strictly by states." Currie, *supra* note 35 at 8.

[1638] Abraha, *supra* note 1521 at 325.

provider offering its service within the country.[1639] Accordingly, the *CLOUD Act* provides an approach that is similar to the "virtual presence" theory found in *Brecknell*, albeit legislatively, rather than by way of the courts. It should be noted that the *CLOUD Act* has also been met with rather strong opposition.[1640]

The "virtual presence" theory also raises important questions about the desirability of using such a technique when considering that reciprocity would need to ensue. In a scenario where the state seeking data found within Canada is not a state with a great human rights record, it can become problematic to allow this foreign state to do so, even if the data that is being accessed does not relate to Canadian citizens. For example, allowing a country that criminalizes homosexuality to remotely gather evidence found in Canada in order to prosecute a 2SLGBTQI+ human rights activist does not seem like something we should simply accept as a society.

Is it possible then to reconcile the positive aspects of the "virtual presence" theory with human rights and general principles on state sovereignty? Recent developments in international law seems to indicate that remote access to data found in another country (or production of the same data by compelling a TPDC) is increasingly seen as a good solution to the investigative problems caused by the internet, even though it is generally agreed that such conduct is contrary to international law, in the absence of a specific agreement between countries.[1641]

[1639] *Ibid* at 336.

[1640] See *inter alia* Bilgic, *supra* note 1594.

[1641] Currie, *supra* note 35 at 17, referring *inter alia* to Susan W Brenner, "Law, Dissonance, and Remote Computer Searches" (2012) 24:1 NC JL & Tech 43–92; Bert-Jaap Koops & Morag Goodwin, "Cyberspace, the Cloud and Cross-Border Criminal Investigation: The Limits and Possibilities of International Law" (2014) Tilburg Institute for Law, Technology, and Society CTLD – Center for Transboundary Legal Development, online:
<https://deliverypdf.ssrn.com/delivery.php?ID=559124089121125007073083097099093124063062077093 05

Indeed, the *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*[1642] was created with the specific intention of providing law enforcement agencies with powers to investigate crimes by collecting transnational digital evidence directly from TPDCs, without having to resort to the MLA process. Further, the *Convention on Cybercrime* itself contains a provision that seems to recognize the relatively low impact that trans-border data collection has on state sovereignty.[1643] Article 32(b) of the *Convention* states that trans-border access to data can be done without the authorization of another party when consent is given by the person that has lawful authority to disclose the data.[1644] This seems to indicate that a TPDC's consent can be sufficient to obtain data stored abroad, without having to go through the MLA process, when the data is identified as been located within the territory of country that is also a party to the *Convention*.[1645] This possibility is however limited by laws that would make it unlawful for

---

403206807501108709010510612000609303309802603804501711907500607406608106712202505900900801809706909109606907008610602300004612510509700809810202511906701709106500403002312311209408207012309807408909202 6&EXT=pdf&INDEX=TRUE>.

[1642] Council of Europe, *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, CETS No 224, 2022. Canada has however not signed the Second additional protocol as of August 2022. Council of Europe, "Chart of signatures and ratifications of Treaty 224", (5 August 2022), online: *Council of Europe* <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224>.

[1643] This provision has however been deemed controversial by some states, namely Slovakia and Russia (who refused to ratify the Convention due to it). See Currie, *supra* note 35 at 16.

[1644] *Convention on Cybercrime*, *supra* note 809 art 32(b).

[1645] The authorized person under this provision could be either the owner of the data (the citizen) or a service provider. See Ronald LD Pool & Bart HM Custers, "The Police Hack Back: Legitimacy, Necessity and Privacy Implications of the Next Step in Fighting Cybercrime" (2017) 25:2 Eur J Crime Crim L & Crim Just 123 at 141. See also Anna-Maria Osula, "Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study" (2016) 24:4 Int'l JL Info & Tech 343 at 352–353, who raises interesting and very valid questions about the applicability and legality of this provision, in light of international law. See also Cybercrime Convention Committee (T-CY), "T-CY Guidance Note # 3 - Transborder access to data (Article 32)", (3 December 2014), online: *Council of Europe* <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726a>.

the TPDC to consent to the production of data to foreign governments.[1646] A recent guidance note pertaining to the *Convention* also seem to embrace the idea that states have jurisdiction to compel the production of data, regardless of the location of the data or the physical presence of the TPDC within its borders.[1647]

In any case, it seems clear that Parliament should address this question directly—rather than leave it to the courts to decide—possibly by signing and ratifying the *Second Additional Protocol to the Convention on Cybercrime,*[1648] by adopting a piece a legislation similar to the US *CLOUD Act*, and potentially by signing bilateral agreements with other countries (including an agreement with the US in order to create reciprocal evidence-gathering authority under the *CLOUD Act* itself, which is currently being negotiated).[1649] The US Supreme Court mentioned during the *Microsoft Ireland* hearings that the issue belonged to Congress, not the Courts,[1650] and this is also true in Canada. If one thing is clear from the *Brecknell* debate is that this innovative approach to the collection of data stored abroad is not unanimously seen as acceptable, especially without clear provisions to this effect. Parliament is in a better position than the courts to craft a framework that considers all the relevant interests at stake

[1646] For example, the American Stored Communications Act allows TPDCs to voluntarily produce non-content data (i.e., metadata) to foreign governments, but prohibits the production of content data when requested outside of the *MLAT* structure. See Abraha, *supra* note 1521 at 328.
[1647] Daskal, *supra* note 1588 at 199–200, referring to Ad-hoc Subgroup on Transborder Access and Jurisdiction, *supra* note 1628.
[1648] It is surprising that this has not already been done, considering Canada played a large part in the drafting of the Second Additional Protocol. See *Evaluation of the Investigative Powers for the 21st Century Initiative - Final Report*, by Justice Canada (Ottawa, Canada: Justice Canada, 2020) at 20.
[1649] Department of Justice - Office of Public Affairs, "United States and Canada Welcome Negotiations of a CLOUD Act Agreement", (22 March 2022), online: *US Department of Justice* <https://www.justice.gov/opa/pr/united-states-and-canada-welcome-negotiations-cloud-act-agreement>.
[1650] Daskal, *supra* note 1626 at 10–11, citing Justice Sotomayor and Justice Ginsburg.

and that reconciles the positive aspects of the "virtual presence" theory with the necessary jurisdictional imperatives. As put by Daskal:

> A test that focuses exclusively on the location of data [i.e., the *NLPC* position] fails to reflect the actual attributes of data in ways that are incongruent with the relevant interests at stake. Conversely, a test that gives law enforcement access to whatever it deems relevant to an investigation, without regard to countervailing considerations [i.e., the *Brecknell* position], is not a satisfactory answer either. […] The goal should be a set of jurisdictional rules that fall in between these two approaches—ones that reflect both the legitimate sovereign interest in sometimes accessing data outside a state's border and the countervailing interests in limiting access to citizens' and residents' data; promote the implementation of baseline substantive and procedural privacy protections; and facilitate user notice with respect to the rules that apply.[1651]

Additionally, Parliament is also in a better position to address some of the issues that the Court in *Brecknell* failed to address, including the consequences of encryption on such collection of data, the impact of term of service agreements that impose a particular forum,[1652] the possible distinction between the collection of content *versus* non-content data,[1653] and the applicability of this theory to lawful hacking techniques that can be used against computers found all over the world.[1654] It could also consider some of the other solutions to this problem that have been suggested over the years, including focusing exclusively on the location or nationality of the

---

[1651] Daskal, *supra* note 1588 at 231.

[1652] As found by Simon Bradshaw, Christopher Millard & Ian Walden, "Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services" (2011) 19:3 Int'l JL Info & Tech 187 at 222, TPDCs will usually include a forum election clause in their terms of service agreements.

[1653] As mentioned by Jennifer Daskal, "Law Enforcement Access to Data across Borders: The Evolving Security and Rights Issues" (2016) 8:3 J of Nat'l Sec L & Pol'y 473 at 485, non-content data (i.e., metadata) usually receives less protection than content data, even though it can increasingly be used to draw a detailed portrait of an individual's life. As such, Parliament should consider whether the same rules should apply to the extraterritorial collection of this data.

[1654] For the jurisdictional considerations of legal hacking techniques, see Brenner, *supra* note 1641; Daskal, *supra* note 1588 at 229–230; Aucoin, *supra* note 147 at 1449–1450; Ghappour, *supra* note 1601.

user.[1655] If the "virtual presence" theory was adopted by Parliament, the impact of using proxy services to change IP address location, a practice that is commonly used to access web services that are not accessible in a specific country or to augment digital privacy,[1656] should also be addressed, considering that the use of these techniques by users basically circumvents a TPDC's decision not to operate in that country, creating a unique problem when it comes to what actually constitutes a "virtual presence" within a country.

In March 2022, Canada and the United States started negotiations in regard to the creation of a bilateral agreement, in accordance with the *CLOUD Act*.[1657] This would essentially remove the need for the use of the "virtual presence" theory for data located within the US or under an American TPDC's control, making Canadian production orders available to obtain data directly from these entities without using the MLA process.[1658] Such a bilateral agreement would effectively resolve the jurisdictional issues related to the collection and production of data in a high number of cases, considering that the most popular TPDCs are found within that country. However, some situations are still likely to occur where law enforcement will need to use the MLA process to obtain the data relevant to an investigation.[1659] The European

[1655] Schiff Berman, *supra* note 1588 at 24–25; Reema Shah, "Law Enforcement and Data Privacy – A Forward-Looking Approach" (2015) 125 Yale LJ 543 at 550.

[1656] Kevin Montgomery, "Proxy Services Are Not Safe. Try These Alternatives", (6 July 2015), online: *Wired* <https://www.wired.com/2015/07/proxy-services-totally-unsecure-alternatives/>.

[1657] Department of Justice - Office of Public Affairs, *supra* note 1640. See also Michael Geist, *David Fraser on Negotiating a CLOUD Act Agreement Between Canada and the United States* (LawBytes Podcast), on the implications of such negotiations for Canada.

[1658] Jessica Jahn, "Canada's Future CLOUD Act Agreement with the United States", (29 March 2022), online: *International Centre for Criminal Law Reform & Criminal Justice Policy ICCLR* <https://icclr.org/2022/03/29/canadas-future-cloud-act-agreement-with-the-united-states/>.

[1659] For example, Abraha, *supra* note 1521 at 335 explain that Microsoft has started using a "data trustee" model that puts the data of its own customers out of reach by handing over control of its datacenters to companies in the country where they are located. This means that Microsoft, if served with a production order, would not be able to produce the data directly and rather a production order would need to be served to the specific trustee in charge of the relevant datacenter.

Commission has also been trying to improve cross-border access to data, including by proposing a new European production order that would allow states to obtain data directly from service providers in a specific timeframe.[1660] The United Nations has also started groundwork that will lead to the drafting of the first UN convention on cybercrime,[1661] which will most likely have impact on transnational data collection and will hopefully resolve some of these issues on a larger scale.

8.3.2 Data Localization Laws

TPDCs will sometimes store data on servers located in proximity to the user's location for technical purposes.[1662] When this is the case and the TPDC has a physical presence in the country that is seeking access to the user's data, the jurisdictional issues explained above are rendered moot: user, TPDC, and law enforcement are all located within the same territorial jurisdiction. However, this will not always be the case, as some TPDCs will not necessarily have (or use) servers located within the user's country or will not have a physical presence within that country. For this reason, some countries have implemented data localization laws

[1660] "E-evidence - Cross-border access to electronic evidence", (2019), online: *European Commission* <https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en>; According to some commentators, a proposal might be coming soon. See "EU: End game approaching for e-evidence negotiations, says French Presidency", (6 July 2022), online: *Statewatch* <https://www.statewatch.org/news/2022/july/eu-end-game-approaching-for-e-evidence-negotiations-says-french-presidency/>. See also explanatory comments in Daskal, *supra* note 1625 at 1039–1043.

[1661] United Nations - Office on Drugs and Crime, "Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes", online: *UNODC* <https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home>. See also Jessica Jahn, "Canada's Position at the UN Cybercrime Treaty Negotiations", (2 March 2022), online: *International Centre for Criminal Law Reform & Criminal Justice Policy ICCLR* <https://icclr.org/2022/03/02/canadas-position-at-the-un-cybercrime-treaty-negotiations/>.

[1662] Abraha, *supra* note 1521 at 337.

in order to avoid the MLA process.[1663] Consequently, this facilitates the acquisition of data by law enforcement for investigative purposes, as any jurisdictional issues are avoided.

Canada has a data localization policy in effect for certain types of governmental data. Following the *Directive on Service and Digital*, computing facilities located within Canada are to be the favored method of storing sensitive information that is categorized as Protected B, Protected C or is Classified.[1664] Data that is unclassified or Protected A does not need to follow any specific data residency regulation.[1665] This is done to ensure the application of Canadian privacy laws and to ensure continuous access to this data for the government in general, not necessarily for law enforcement purposes.[1666] Canada does not have any data localization law when it comes to the location of data held by private sector TPDCs.

There are multiple downsides to data localization laws. First, these laws only work when a TPDC actually knows the user's physical location, which will not always be the case. For example, it seems that Microsoft does not verify users' location, but rather trusts what the user provides as a country of residence at the moment of sign-up.[1667] Second, data localization laws can facilitate governmental collection of data to the point that privacy and civil rights are being infringed.[1668] Third, technological and logistical considerations can also make these impractical for TPDCs, as these laws effectively compel them to build and operate new data

---

[1663] Daskal, *supra* note 1653 at 473; Jonah Force Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders" (2014) Hague Inst Glob Just Conf Future Cyber Gov at 3.

[1664] Government of Canada, "Directive on Service and Digital", (6 May 2022), online: *Government of Canada* <https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32601>, s 4.4.3.14.

[1665] Government of Canada, "Guideline on Service and Digital", (23 November 2021), online: *Government of Canada* <https://www.canada.ca/en/government/system/digital-government/guideline-service-digital.html>.

[1666] *Ibid*.

[1667] Abraha, *supra* note 1521 at 338.

[1668] Barton, *supra* note 1626 at 97.

centers all over the world, even in places unsuitable for such energy consuming activity.[1669] In turn, this would likely create an increase in costs for TPDCs and in prices for consumers.[1670] Fourth, data localization laws are also in general opposition with the aim and functioning of the internet. Restricting the flux of internet data necessarily impacts the efficiency of the internet and the "free exchange of ideas and information."[1671] As stated by one author, jurisdictional rules should change to fit the realities of human activities, not the other way around.[1672] As there seems to be a general consensus against the adoption of data localization laws, Canada should refrain from considering this alternative as a good solution to the jurisdictional issues caused by the delocalization of data, at least for law enforcement purposes.

[1669] Experts mention that data centers should be located in places where the outside air is no higher than 27 degrees Celsius. Chris Stokel-Walker, "Data Centers Are Facing a Climate Crisis", (1 August 2022), online: *Wired* <https://www.wired.com/story/data-centers-climate-change/>.

[1670] Daskal, *supra* note 1588 at 227; Daskal, *supra* note 1653 at 477.

[1671] Vivek Krishnamurthy, "Cloudy with a Conflict of Laws" (2016) Berkman Klein Cent Internet Soc Res, online: <https://dash.harvard.edu/bitstream/handle/1/28566279/SSRN-id2733350.pdf?sequence=1&isAllowed=y> at 9, cited in Bilgic, *supra* note 1594 at 346. See also Daskal, *supra* note 1653 at 473; Force Hill, *supra* note 1663 at 4.

[1672] Schiff Berman, *supra* note 1588 at 23–24.

PART 3 – ACCESS TO DATA IN TRANSIT

CHAPTER 9 THE IMPACT OF ENCRYPTION ON THE INTERCEPTION OF PRIVATE COMMUNICATIONS

As part of Parliamentary oversight of the use of Part VI of the *Criminal Code*, which regulates electronic surveillance of private communications, a yearly report must be produced by the Minister of Public Safety and Emergency Preparedness.[1673] In the 2020 report, the Minister reported a decrease in applications from law enforcement agencies for the use of electronic surveillance.[1674] This might indicate that this technique remains exceptional in its use. Conversely, it could also indicate that law enforcement agencies will refrain from applying for a Part VI authorization when they know that they will not be able to enforce it because of the use of end-to-end encryption by the targets.[1675]

End-to-end encryption (E2EE)—which is used by many communication service providers, such as *WhatsApp*, *Skype*, *Signal*, and other Voice over Internet Protocol (VoIP) services—is making wiretapping impossible for law enforcement, even with the required court authorizations.[1676] As put by Anne Turner:

[1673] *Criminal Code*, *supra* note 37, s 195.

[1674] Public Safety Canada*, 2020 Annual Report on the Use of Electronic Surveillance* (Public Safety Canada, 2021) at 5.

[1675] Nicholas Koutros & Julien Demers, "Big Brother's Shadow: Decline in Reported Use of Electronic Surveillance by Canadian Federal Law Enforcement" (2013) 11 CJLT at 111–112. See also Christopher Parsons & Adam Molnar, "Government Surveillance Accountability: The Failures of Contemporary Canadian Interception Reports" (2018) 16 CJLT 143 at 166, who criticize the value of these annual reports, *inter alia* because they fail to provide useful narratives linked to the use of wiretap authorizations, including the number of instances where electronic surveillance could not be conducted because of encryption.

[1676] Chan & Aylward, *supra* note 298 at 4; Etzioni, *supra* note 25 at 566; Opderbeck, *supra* note 3 at 1661; *R v Williams*, 2014 NBJ 356.

> Part VI authorizations would be capable of including the interception and decryption of encrypted communications if legislation required service providers to retain decryption information. If law enforcement possessed a valid wiretap authorization that included an assistance order, requiring a service provider to retain decryption keys and provide those to law enforcement, then a wiretap authorization would be capable of covering encrypted messages. The true problem arises in that service providers are not required by legislation to retain such information and therefore do not have it to provide to law enforcement. As such, the ability of law enforcement to intercept some communications is thwarted, even when they are in the possession of a wiretap authorization for which they have had to establish all the statutory preconditions to the satisfaction of the issuing justice.[1677]

Indeed, Chan and Aylward report that the WhatsApp encryption system "has stymied the ability of law enforcement to execute wiretap authorisations and has led to a dispute with the company."[1678] In a similar manner, some companies do not only offer software that promises to keep prying ears from conversations, but also hardware (mostly phones) that are modified to ensure that law enforcement cannot track the device and cannot intercept the communications made on it, voice or text.[1679] The mathematical functioning of computers can also make it challenging to distinguish data and voice communications when the

[1677] Turner, *supra* note 863 at 291.

[1678] Chan & Aylward, *supra* note 298 at 4.

[1679] For example, Phantom Secure and Encrochat both offered phones designed to avoid any type of surveillance. Encrochat's network was however eventually hacked by law enforcement in a massive operation. Joseph Cox, "The FBI Tried to Plant a Backdoor in an Encrypted Phone Network", (18 September 2019), online: *Vice* <https://www.vice.com/en_ca/article/pa73dz/fbi-tried-to-plant-backdoor-in-encrypted-phone-phantom-secure>; Mike Corder, "European police crack encrypted phones, arrest hundreds", *Washington Post* (2 July 2020), online: <https://www.washingtonpost.com/world/europe/french-dutch-police-bust-encrypted-criminal-communications/2020/07/02/ff664844-bc55-11ea-97c1-6cf116ffe26c_story.html>.

communications are made using VoIP services,[1680] further complicating the work of law enforcement.

Following the Supreme Court of Canada's decision in *R v TELUS Communications Co*, a Part VI authorization is required not only for the interception of voice calls, but also for text messages intercepted in real time or in a prospective manner.[1681] It is also the appropriate authorization to intercept emails.[1682] When telecommunication service providers have implemented encryption measures themselves, they are required to give law enforcement access to conversation *en clair* (meaning in its decrypted form), when presented with the necessary court order.[1683] However, this obligation has been interpreted as not applying to internet-based communications,[1684] and there exists no general obligation on telecommunications companies to facilitate wiretapping.[1685] Further, users can also add their own encryption software and some companies are unable to circumvent their own encryption measures by design.[1686] Thus, encryption has the potential to hinder the interception of multiple communications, especially in light of the findings from Chapter 8, where it was argued that TPDCs should not be mandated to include exceptional access mechanisms into their systems, due to technical, policy, and rights-based arguments.

[1680] Daniel B Garrie, Matthew J Armstrong & Donald P Harris, "Voice over Internet Protocol and the Wiretap Act: Is Your Conversation Protected?" (2005) 29:1 Seattle U L Rev 95 at 95.
[1681] *TELUS*, *supra* note 249.
[1682] *R v Merritt*, *supra* note 791; Alan D Gold, "If the shoe fits... and wonderfully so: Part VI of the *Criminal Code* Should be Applied to Digital Communications" (2016) ADGN at para 11.
[1683] Penney & Gibbs, *supra* note 3 at 217–218. For more details, see Section 10.1 *infra*.
[1684] *Ibid* at 218 citing Parsons, *supra* note 66.
[1685] Chan & Aylward, *supra* note 298 at 9.
[1686] See for example SpiderOak, "No Knowledge, Secure-by-Default Products", online: <https://spideroak.com/no-knowledge/>.

It is clear that the *Charter* does not include a right to absolute privacy. If such a right existed, we would not have any court order that allows law enforcement to access private information. Therefore, when all the conditions to obtain a wiretap order—or any other court order for that matter—are satisfied, it seems intuitively right to give law enforcement some way of effectively enforcing the order, if only because the privacy rights have already been considered under the requirements that must be met by law enforcement in order to obtain the judicial order. However, and as seen previously, experts agree that any method used to compel service providers to maintain decryption capacity are inherently insecure and put the privacy of innocent users at risk.[1687] How is it possible then to reconcile law enforcement's interest in accessing communications in real time, using wiretaps, with the fact that strong encryption is necessary, has so many positive applications, and should not be weakened?

This chapter will explore these considerations and suggest that the solution to this problem is likely to be found in the use of lawful hacking techniques by law enforcement. It will also be suggested that acquisition of metadata by law enforcement can alleviate at least partly the absence of wiretapping capacities in some instances. The jurisdictional considerations linked to this issue will also be touched upon.

9.1 The Impact of Encryption on the Interception of Private Communications

Prior to the advent of electronic communications, permanent recordings of conversations were uncommon; absent a pre-existing wiretap authorization, only letters provided a record of a communication, albeit in a disjointed and less conversational way.[1688] Nowadays, a multitude

[1687] See Chapter 8.

[1688] Steven Penney, "Consent Searches for Electronic Text Communications: Escaping the Zero-Sum Trap" (2018) 56 Alta L Rev 1 at paras 1–2.

of communications platforms exist and are used in place of phone calls, creating nearly permanent records of highly private communications.[1689] Individuals are increasingly relying on these to engage with their peers in novel ways,[1690] without thinking about the digital traces they are simultaneously creating.

In light of the Snowden revelations and other incidents where users' private information was made public, there has been a rise in E2EE and a movement towards perfect forward secrecy.[1691] It seems that in Canada in 2018, approximately 70% of intercepted communication were encrypted.[1692] There might be a resurgence in interest towards encrypted communications following the overturning of *Roe v Wade* in the United States and the subsequent discovery that Facebook communicated data to the authorities in a case involving an alleged illegal abortion.[1693]

[1689] As put by Gerald Chan, "Text Message Privacy: Who Else Is Reading This?" (2019) 88 SCLR (2d) 69 at 74, "[e]ven if we delete messages from our devices, they can be recovered forensically." In reference to *Vu*, *supra* note 1 at para 43.

[1690] It is safe to say that prior to the advent of digital communications and their fairly recent expansion to allow video conversations and the rapid exchange of videos and photos files, practices such as "sexting" had no analog equivalent. Accordingly, digital communications technologies have created a new way of engaging with others, in a manner that demonstrates a high subjective expectation of privacy. This expectation of privacy is highly dependent on the privacy protection measures put in place by service providers (i.e., the more secure a service is perceived to be, the more revealing the communications are likely to be). For this reason, it is debatable if electronic communications are the equivalent of telephonic communications. It seems like electronic communications are rather a new type of communication, one that is halfway between physical interactions and textual communication. See *Marakah*, *supra* note 260 at paras 34–37, in which the majority acknowledged the unique nature of electronic conversations.

[1691] Abelson et al, *supra* note 3 at 12.

[1692] West & Forcese, *supra* note 85 at 4.

[1693] Lily Hay Newman, "End-to-End Encryption's Central Role in Modern Self-Defense", (5 July 2022), online: *Wired* <https://www.wired.com/story/end-to-end-encryption-abortion-privacy/>; Johana Bhuiyan, "Facebook gave police their private data. Now, this duo face abortion charges", (10 August 2022), online: *The Guardian* <https://www.theguardian.com/us-news/2022/aug/10/facebook-user-data-abortion-nebraska-police>.

As mentioned in Chapter 2, E2EE is a method that protects data in transit by using public key cryptography (also called asymmetric encryption), making the contents of a communication indecipherable to third parties. The caveat with E2EE is that once an attacker obtains the encryption key, the entirety of the previous and future communications will be decipherable.[1694] This has led law enforcement to store intercepted but undecipherable communications on servers, in the hopes of obtaining the encryption key in the future.[1695] Perfect forward secrecy addresses this issue by enhancing the protection given by E2EE. It "automatically and frequently changes the keys it uses to encrypt and decrypt information, such as if the latest key is compromised, it exposes only a small portion of the user's sensitive data."[1696] For example, the Signal messaging application uses perfect forward secrecy, as does WhatsApp.[1697] Both E2EE and perfect forward secrecy are currently preventing law enforcement from accessing intercepted messages *en clair*.[1698]

In this context, law enforcement has been trying to retain its interception capacities,[1699] mostly by advocating for regulation to be imposed upon service providers. Currently,

---

[1694] Greenberg, *supra* note 161.

[1695] Gill, Israel & Parsons, *supra* note 3 at 8. The same technique of waiting on technological advancements to circumvent encryption is also applied to data at rest. See for example *R v McBride*, 2017 BCSC 1016 at para 8; and *R v Seguin*, 2015 ONSC 1908, in which the Court determined that encryption could be a motive to extend the usual period of detention for seized objects, under s. 490 of the *Criminal Code*.

[1696] Greenberg, *supra* note 161.

[1697] Sarah Lewis, "Perfect forward secrecy (PFS)", (September 2018), online: *TechTarget* <https://www.techtarget.com/whatis/definition/perfect-forward-secrecy>.

[1698] In other words: "[e]ncryption of the data does not itself prevent a wiretap from intercepting the communication, but without the key, the wiretapper cannot understand what is being said." Opderbeck, *supra* note 3 at 1661.

[1699] Valerie Caproni, general counsel for the FBI, has stated that the state is not trying to gain more powers in this context, but simply to maintain its current investigative powers. See Lowell, *supra* note 221 at 506. This seems to also be the prevalent position in Canada. However, it could be argued that giving law enforcement access to electronic communications *en clair* would indeed give law enforcement more powers, as the amount of information they could gather in this manner has no historical equivalent.

communications service providers have some obligations when it comes to encryption, as per Standard twelve of the *Solicitor General's Enforcement Standards* (SGES).[1700] The SGES, described by West and Forcese as a "narrower and less transparent administrative instrument [as opposed to formal statutory decryption obligations],"[1701] were established in the 1990s and wireless communications service providers are required to implement them to receive a license to operate in Canada.[1702] According to this norm, mobile service providers must be able to provide law enforcement with intercepted communications *en clair*, if they initiated the encryption themselves.[1703] Otherwise, "there is no law in Canada designed to require a person or organization to decrypt their communications."[1704]

Standard twelve of the SGES does not, however, prohibit the deployment of E2EE by service providers, which significantly limits the scope of the Standard,[1705] as E2EE inherently removes the possibility for the service provider to access the data in its decrypted form. Further, this obligation currently only applies to wireless telecommunications providers, although there have been some discussions in the past to expand the SGES to other service

[1700] A copy of the SGES can be found at CIPPIC, "Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications – Compliance Table" (17 November 2008), online: Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic <https://www.cippic.ca/uploads/ATI-SGES_Annotated-2008.pdf>. Parsons & Israel, *supra* note 167.

[1701] West & Forcese, *supra* note 85 at 11. According to the authors, "the terms of the SGES are not public. It is our understanding that the most recent version was updated in 2015. However, the only published version of the SGES – of which we are aware – dates to 2008 and was obtained by a Canadian newspaper through a freedom of information request." (References from the original omitted.)

[1702] Parsons, *supra* note 66 at 34.

[1703] Parsons & Israel, *supra* note 167; Parsons, *supra* note 66 at 34.

[1704] Public Safety Canada, *supra* note 79 at 61. See also Gill, Israel & Parsons, *supra* note 3 at 37.

[1705] Gill, Israel & Parsons, *supra* note 3 at 60.

providers, including internet-based telecommunications service providers.[1706] This means that third-party VoIP or texting applications are not subject to the SGES.[1707]

The issues related to the impact of encryption on wiretapping capacities are not directly related to the rights and freedoms found in the *Charter* per se. Indeed, these are already considered by the courts when they are examining if the Part VI authorization should be granted to law enforcement.[1708] Additionally, the technical method used by law enforcement is usually found to be out of the scope of a s. 8 analysis, to the extent of being deemed reasonable under the *Collins* analysis.[1709] Rather, this is mostly a policy issue, with some impact on third parties' privacy rights (as opposed to the privacy rights of the person under investigation).

9.2 Potential Solutions

While a compelled decryption regime such as the one suggested in Chapter 7 has the potential to solve the problem of encryption for data at rest, it does nothing to solve the problem of access to data in transit.[1710] Without access to the encryption key, law enforcement will be able to intercept the communications, but will not be able to read them, even with the appropriate wiretap authorization under Part VI of the *Criminal Code*. While a s. 487.02

[1706] Geist, *supra* note 1348 at 268; Gill, Israel & Parsons, *supra* note 3 at 61. As per Fehr, *supra* note 319 at 104, this idea was however abandoned by the government, in light of objections made by telecommunications service providers. West & Forcese, *supra* note 85 at 12–13.

[1707] Parsons & Israel, *supra* note 167.

[1708] As explained in Chapter 7 *supra*, encryption by itself does not create an inviolable sphere of privacy that law enforcement cannot try to penetrate. Although compelled decryption implicates a higher expectation of privacy because of the involvement of the principle against self-incrimination, absent the compulsion, s. 8 of the *Charter* sufficiently addresses the privacy aspect of encryption and of digital data.

[1709] *R v Collins*, *supra* note 31.

[1710] Penney & Gibbs, *supra* note 3 at 229.

assistance order has the potential of being used to compel assistance from a service provider, as seen in Chapter 8,[1711] it is uncertain if it could be used in a situation where the encryption mechanism makes assistance impossible.[1712]

In 2015, it was revealed that the RCMP had gained access to the global decryption key for BlackBerry devices, allowing them to intercept thousands or messages that were thought by the suspects to be encrypted in such was as to be perfectly secure.[1713] The Crown did not want to disclose how it got access to such highly confidential information, *inter alia* because of the negative impact it could have on Research in Motion (RIM), the company that manufactured BlackBerry devices at the time.[1714] It was also feared that the key, if it fell into the wrong hands, could be used illegitimately to decipher any message sent using a BlackBerry device.[1715] Ultimately, the Quebec Superior Court determined that the role of RIM in the interception and decoding process, including the encryption key, was to be disclosed to the accused individuals, under the right to a full answer and defence.[1716] In turn, this led to a stay of proceedings being entered against the 11 charged men, as the Crown refused to disclose the information.[1717] Accordingly, it is currently unknown if the RCMP had obtained RIM's

---

[1711] See also West & Forcese, *supra* note 85 at 15.

[1712] For example, it has been reported that Facebook successfully contested a wiretapping request that would have required the circumvention of its own encryption methods. See Chaim Gartenberg, "Facebook reportedly avoids US government wiretap of Messenger voice calls", (28 September 2018), online: *The Verge* <https://www.theverge.com/2018/9/28/17915902/facebook-messenger-protected-us-government-wiretap-requests>.

[1713] *Mirarchi I*, *supra* note 300 at para 43. It also seems like Apple gave access to its decryption key to the authorities in China. See Bilgic, *supra* note 1594.

[1714] *Mirarchi I*, *supra* note 300 at para 45.

[1715] Jordan Pearson & Justin Ling, "Exclusive: How Canadian Police Intercept and Read Encrypted BlackBerry Messages - VICE", (14 April 2016), online: <https://www.vice.com/en_us/article/mg77vv/rcmp-blackberry-project-clemenza-global-encryption-key-canada>.

[1716] *Mirarchi I*, *supra* note 300 at paras 288–289.

[1717] Paul Cherry, "Montreal Mafia: Project Clemenza screeches to a halt as cases stayed", (17 July 2017), online: *Montreal Gazette* <https://montrealgazette.com/news/local-news/montreal-mafia-project-clemenza-screeches-

assistance voluntarily or following the issuance of an assistance order.[1718] It seems clear then that more sustainable and transparent investigation techniques that allow for the interception of encrypted private communications must be found.

As seen in Chapter 8, key escrow mechanisms were suggested as a solution to the "going dark" problem back in the 1990s and made a reappearance in the public debate recently.[1719] However, when it comes to data in transit that is protected by perfect forward secrecy, key escrow is inapplicable.[1720] As put by Abelson et al.: "all known methods of achieving third-party escrow are incompatible with forward secrecy,"[1721] due to the fact that this type of encryption generates new keys on a regular basis. Thus, this solution is not sufficient to address the concerns raised by law enforcement, especially in a context where a criminal would most likely switch to systems using perfect forward secrecy if key escrow was imposed on communication service providers using 'regular' E2EE.

The comments made in Chapter 8 as to the negative impacts of trying to regulate and limit encryption at the source apply essentially identically when it comes to data in transit. Encryption, whether for data at rest or data in transit, is necessary and important at multiple levels, including for the exercise of rights and freedoms, from a cybersecurity perspective, and for economic reasons.[1722] Limiting encryption capacities for data in transit would unduly

---

to-a-halt-as-cases-stayed#:~:text=A%20lengthy%20investigation%20into%20drug,against%20them%20only%20last%20year.>; West & Forcese, *supra* note 85 at 2.

[1718] Gill, Israel & Parsons, *supra* note 3 at 58.

[1719] See for example Corn, *supra* note 296 at 341; Opderbeck, *supra* note 3 at 1681.

[1720] Opderbeck, *supra* note 3 at 1667.

[1721] Abelson et al, *supra* note 3 at 12.

[1722] See Chapters 2 and 8, and also generally Parsons, *supra* note 56.

affect law-abiding citizens,[1723] in a manner that does not strike an appropriate balance between individual privacy rights and the state's obligation to investigate crimes and prosecute criminals, as required by ss. 7 and 8 of the *Charter*, and in last recourse under s. 1. Suggestions to simply ban E2EE[1724] are naïve in light of how the internet actually functions and do little to advance the debate in a helpful manner, as they do not recognize the systemic impacts such a measure would have on uninvolved parties or acknowledge the positive impacts of strong encryption. Accordingly, the solution to the "going dark" problem applied to data in transit must be found elsewhere.[1725]

9.2.1 Using Lawful Hacking Techniques to 'Intercept' Private Communications

Lawful hacking techniques are increasingly seen as the most viable solution to the encryption of electronic communications.[1726] These techniques are also useful when the location of a device is unknown to law enforcement. As explained by Ahmed Ghappour:

> Network investigative techniques [i.e., 'lawful hacking' techniques] create a way for investigators to reach a computer that does not require knowledge of its physical location. Rather than traversing "physical" pathways—such as roads and bridges—to reach the target's physical address, investigators deploy malware that traverses "virtual" pathways—such as connections between computers and bridges between networks—to reach the computer's virtual IP address. Importantly, the new methods

[1723] As put by Gill, Israel & Parsons, *supra* note 3 at 35, "there is simply no practical way to weaken or undermine encryption technology without compromising that technology for all users."
[1724] See for example Etzioni, *supra* note 25.
[1725] Not discussed here is the possibility of accessing communications *after* they have arrived at their destination, in other words when *data in transit* is transformed into *data at rest* (see Part 2 of this thesis). While this could indeed be an alternative to obtain communications in their decrypted form, it does not serve the same purpose as wiretapping. As such, it is of limited help when law enforcement is trying to access data in real time.
[1726] Liguori, *supra* note 70 at 328; West & Forcese, *supra* note 85 at 17; Wainscott, *supra* note 1460 at 75; Bellovin, Blaze & Landau, *supra* note 197 at 5; Dheri & Cobey, *supra* note 77 at 19.

> can reach the same destination. Once malware penetrates the target, it converts the computer into a surveillance device.[1727]

As seen previously, both the United States and the UK have started using lawful hacking to circumvent encryption. While the use of these techniques by law enforcement prompts some questions that have not been yet addressed by Canadian courts or Parliament, it is possible for them to provide an adequate balance between law enforcement's interest in investigating and combatting crime and law-abiding citizens' interest in protecting their privacy. The use of lawful hacking techniques has the advantage of not creating a systemic vulnerability in communications systems, which would unduly impact uninvolved parties.

The use of a keylogging (also called keystroke) software could be a viable alternative to the interception of private communications, when encryption prevents law enforcement from accessing the communications *en clair*. It would allow for the interception of the communication, before it is turned into ciphertext.[1728] The use of this technique would require a Part VI authorization, as it would give law enforcement access to communications typed by the owner of a device in real time.[1729] The use of a *Trojan horse* might also yield similar results.[1730] However, this might require us to rethink the definition of the term 'intercept,' due to the fact that the keylogger software or *Trojan horse* would allow law enforcement to obtain the content of the communication immediately before it is sent by the target, rather than while

[1727] Ghappour, *supra* note 1601 at 1096.
[1728] Opderbeck, *supra* note 3 at 1662.
[1729] Hubbard, Brauti & Fenton, *supra* note 853, s 6:38.
[1730] "A Trojan horse, or Trojan, is a type of malicious code or software that looks legitimate but can take control of your computer. [...] [A remote Access Trojan] can give an attacker full control over your computer via a remote network connection. Its uses include stealing your information of spying on you." Alison Grace Johansen, "What is a Trojan? Is it a virus or is it malware?", (24 July 2020), online: *Norton* <https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html>.

it is transiting on a network.[1731] The United States Supreme Court, for example, concluded that the use of a keylogger program did not constitute an intercept because it acquired the typed text before it was sent on a network.[1732]

Conceiving the term 'intercept' to include such acquisition of communications would likely be unproblematic in light of *TELUS*, in which the SCC equated the technique used by law enforcement to a wiretap, because it had been used to secure the prospective and continual delivery of future communication.[1733] This would also be the case with a keylogger. Thus, the use of a keylogger or any other type of similar malware to obtain a communication as it is typed by a target is entitled to receive the same level of protection as the message that is sent a mere few moments later.

9.2.2 Resorting to Metadata as an Investigative Alternative

While the contents of communications can be encrypted using either E2EE or perfect forward secrecy, a lot of information related to the communications will usually remain unencrypted, and thus accessible from a service provider.[1734] This metadata,[1735] while seemingly innocuous, can reveal a lot of information about a person, especially once combined with other information.[1736] The sheer amount of metadata is increasing, due to the fact that individuals

---

[1731] Fehr, *supra* note 319 at 98; Steven Penney, "Updating Canada's Communications Surveillance Laws: Privacy and Security in the Digital Age" (2008) 12 Can Crim L Rev 115 at 126.
[1732] Penney, *ibid* at 127.
[1733] *TELUS*, *supra* note 249 at para 67.
[1734] Penney, *supra* note 1731 at 143.
[1735] As mentioned previously, communications metadata is "information about communications data, separate from the communication content itself. This category of information may include: device location data, IP address of the sender and receiver of the communications, telephone calling records, and more." See Liguori, *supra* note 70 at 326.
[1736] Gill, Israel & Parsons, *supra* note 3 at 9.

now own more and more digital devices, including Internet of Things (IoT) devices,[1737] each of them creating metadata that can be amalgamated to create a vivid portrait of users' lives.

Law enforcement can obtain most metadata with production orders, which requires them to satisfy a lower burden of proof than what is required to intercept the contents of the communications. Indeed, the different production orders found in the *Criminal Code* that are applicable to the obtention of metadata[1738] use the lower standard of "reasonable grounds to suspect," rather than "reasonable grounds to believe" that is applicable for the obtention of a Part VI authorization. Accordingly, this provides an interesting alternative for law enforcement that can be used at an earlier stage of an investigation. If this is perceived as a viable alternative by Parliament, retention obligations for certain metadata could be imposed upon service providers.[1739] In the meantime, law enforcements agencies can resort to ss. 487.012 or 487.013 of the *Criminal Code* that both allow for the preservation of data, if necessary.

Some weaknesses exist with this alternative, however. First, while there is indeed more and more unencrypted metadata available, it will not necessarily correspond with what would have been obtained through a Part VI authorization.[1740] Second, metadata from users of anonymization tools such as TOR will be very limited and will not be useable to draw conclusions about the individuals behind the keyboard, as the type of encryption used by TOR prevents law enforcement from being able to access communications in real time and will

[1737] Additionally, IoT devices are usually prone to security issues (Liguori, *supra* note 70 at 327–328), making them an interesting entry point into a network for law enforcement using lawful hacking techniques.
[1738] See Section 5.3.1(C) *supra*.
[1739] Hurwitz, *supra* note 69 at 417–418.
[1740] *Ibid* at 401.

hide metadata for third parties.[1741] Finally, until Big Data analytics become more mundane in law enforcement's arsenal of techniques, it will continue to be quite burdensome and consumptive of time and resources to analyze metadata.

9.3 Jurisdictional Issues Linked to the Interception of Private Communications

9.3.1 Issues Related to the Provisions Found in the Criminal Code

In addition to the issues linked to the delocalization of data mentioned in Chapter 8, the interception of internet-based encrypted private communications raises unique jurisdictional concerns. Part VI of the *Criminal Code* is made applicable to communications within Canada, as per the definition of private communications found in s. 183. Further, ss. 184.2(4)(c), 185(1)(e), and 186(4)(c) also require law enforcement to specify and describe the place where the interception will be conducted. While these requirements were previously satisfied with ease by law enforcement, due to the static nature of landlines, the advent of wireless electronic communications—either using cell phones or internet-based communications platforms—has removed any certainty when it comes to a user's physical location.[1742] Finally, if trying to use an assistance order under s. 487.014 of the *Criminal Code* to obtain assistance from a service provider to decrypt communications in transit, the enforceability of such order on a service provider located abroad without going through the *Mutual Legal Assistance* (MLA) process remains unanswered as of yet.[1743]

[1741] Ghappour, *supra* note 1601 at 1087.
[1742] Turner, *supra* note 863 at 260–263.
[1743] West & Forcese, *supra* note 85 at 16. See also Chapter 8, *supra*.

As put by Anne Turner, "constraining law enforcement to intercept only communications originated or intended to be received in Canada is no longer realistic with current and emerging technology."[1744] However, removing the requirement completely would likely offend principles of sovereignty and territoriality.[1745] Turner suggests focusing on the location of the offence under investigation, rather than on the location of the parties to a communication.[1746] Other authors have suggested that the place of the intercept can also include the place from which law enforcement listens to the intercepted communication, at least when one of the parties to the communication is located on Canadian soil,[1747] which effectively removes the problem in many situations, albeit no in all.

9.3.2 Issues Related to the Use of Lawful Hacking Techniques

As with the decryption of data at rest, the use of lawful hacking techniques to circumvent encryption of data in transit raises jurisdictional questions. If indeed law enforcement is resorting to lawful hacking as a method of avoiding being stalled by encryption applied to data in transit, then the jurisdictional friction comes from the fact that such techniques can allow law enforcement to access devices that are found anywhere in the world, sometimes without even knowing that they are conducting a cross-border search. Indeed, the use of the dark web and of private networks such as TOR can provide perfect anonymity to users, as well as hiding any trace of their location.[1748] Proxy servers can also be used to hide a user's

[1744] Turner, *supra* note 863 at 262–263.
[1745] *Ibid* at 263.
[1746] *Ibid*.
[1747] Hubbard, Brauti & Fenton, *supra* note 853, s 6:22.
[1748] Ghappour, *supra* note 1601 at 1087.

location,[1749] making it virtually impossible for law enforcement officials to know exactly where a monitored device is located.

In the United States, the Federal Rule of Criminal Procedure 41 explicitly allows for the use of lawful hacking techniques when "the location of the target data or device is unknown and the location has been concealed due to technological means, such as the use of anonymization software like Tor."[1750] While the US Department of Justice stated that the rule was not adopted with the intent of allowing extraterritorial searches, it seems unavoidable that this will be the case, especially in a context where the lawful hacking techniques would be used to uncover users of the dark web, which are likely to be located outside of the US.[1751] The Rule's extraterritorial application has been widely criticized.[1752]

Following the requirements put forth by the SCC in *Hape* when it comes to the extraterritorial application of Canadian legislation, which state that "Canadian criminal legislation is territorial unless specifically declared to be otherwise,"[1753] a similar provision would need to be adopted in order for lawful hacking techniques to be deployed by law enforcement on targets located abroad. Even then, this might be conceived as an interference and violation of international law on sovereignty and territoriality,[1754] at least when a government is made aware of the extraterritorial location of a device and continues to search it regardless.[1755] As

[1749] *Ibid* at 1088.
[1750] Daskal, *supra* note 1588 at 205.
[1751] Ghappour, *supra* note 1601 at 1081.
[1752] Including by the Electronic Frontier Foundation and Google. *Ibid* at 1082.
[1753] *R v Hape*, *supra* note 1608 at para 67.
[1754] Ghappour, *supra* note 1601.
[1755] Daskal, *supra* note 1588 at 207–208.

such, it has been suggested that governments should seek consent from foreign states when the location of the target's device is known to be located within their territory.[1756]

Alternatively, it could be argued that lawful hacking techniques do not impede on another state's sovereignty if the location of the search is deemed to be the location of the computer from which the authorities conduct their attack, rather than the targeted device's location. This would not only remove the extraterritoriality issue but also make the *Charter* applicable to the search.[1757] It has also been argued that cross-border computer searches are not prohibited under customary international law.[1758] However, in light of growing international consensus as to the extra-territorial nature of cross-border searches of digital evidence, this is unlikely to be accepted widely at an international level, in the absence of clear guidance on this subject emanating from international legal instruments or from customary international law.[1759] Nevertheless, when the location of the targeted device is unknown because of concealment technologies being used by the target, qualifying the location of the search as being the location of law enforcement's computer, effectively removing a potential jurisdictional debate, seems like an adequate proposition,[1760] especially since no other state will be able to prove that the search occurred on their territory.[1761]

[1756] Jennifer Daskal, "Transnational Government Hacking" (2020) 10:3 J Natl Secur Law Policy 677 at 679.
[1757] *R v Hape*, *supra* note 1608 at para 85; Bercovitz, *supra* note 1455 at 1255.
[1758] John Douglass, "The Legality of Watering-Hole-Based NITs under International Law" (2017) 2:1 Geo L Tech Rev 67 at 78; Orin S Kerr & Sean D Murphy, "Government Hacking to Light the Dark Web: What Risks to International Relations and International Law?" (2017) 70 Stan L Rev Online 58.
[1759] See Chapter 8 *supra*.
[1760] Bercovitz, *supra* note 1455 at 1283. See also Douglass, *supra* note 1758 at 78, who states that some authors have opined that "a unilateral cross-border search will not necessarily violate customary international law when law enforcement does not know where the computer is located prior to conducting the search."
[1761] A foreign country would most likely only be aware that such search occurred on their territory when that information is made public at trial.

It has recently been reported that a powerful spyware named Pegasus, developed by the company NSO Group, had been used to infect the devices of various individuals and monitor their messages, including US Embassy employees,[1762] journalists,[1763] individuals related to Jamal Khashoggi,[1764] and political activists.[1765] First discovered by the Citizen Lab in 2021,[1766] the use of Pegasus demonstrates that hacking—whether lawful or not—knows no boundaries. Indeed, individuals located in many different countries were targeted by the attacks, while the countries having hired the Israel-based firm to conduct them are still unknown.[1767]

Pegasus, which was developed to help "government intelligence and law enforcement agencies use technology to meet the challenges of encryption,"[1768] further demonstrates that lawful hacking, while indeed a potential solution to the "going dark" problem, is not immune to abuses and requires strict supervision in order to be used in a manner that does not offend the international rules on comity and state sovereignty, in addition to internationally

---

[1762] Craig Timberg, Drew Harwell & Ellen Nakashima, "NSO Pegasus spyware used to hack U.S. diplomats working abroad", (3 December 2021), online: *Wash Post* <https://www.washingtonpost.com/technology/2021/12/03/israel-nso-pegasus-hack-us-diplomats/>.

[1763] Mitchell Clark, "NSO's Pegasus spyware: here's what we know", (23 July 2021), online: *The Verge* <https://www.theverge.com/22589942/nso-group-pegasus-project-amnesty-investigation-journalists-activists-targeted>.

[1764] *Ibid*. Jamal Khashoggi was a journalist and critic of the Saudi Arabia's government, who was murdered at the Saudi consulate in Istanbul on September 28, 2018. See "Jamal Khashoggi: All you need to know about Saudi journalist's death", (24 February 2021), online: *BBC News* <https://www.bbc.com/news/world-europe-45812399>.

[1765] Joseph Menn, "Dozens of Thai activists and supporters hacked by NSO Group's Pegasus", (17 July 2022), online: *Washington Post* <https://www.washingtonpost.com/technology/2022/07/17/pegasus-nso-thailand-apple/>.

[1766] Bill Marczak et al, "FORCEDENTRY - NSO Group iMessage Zero-Click Exploit Captured in the Wild", (13 September 2021), online: *Citizen Lab* <https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/>.

[1767] Clark, *supra* note 1763.

[1768] *Ibid* citing the NSO Group's website.

recognized individual rights and freedoms. It is outside the scope of the current proposals to identify a specific set of tools that would deal with the international law issues, but they will need to be considered.

CHAPTER 10 CONCLUSION

Irgvctxmsr...mw e tsaivjyp hijirwmzi aietsr jsv jvii tistpi. Mx sjjivw e xiglrmgep kyeverxii sj tvmzegc, vikevhpiww sj als mw vyrrmrk xli kszivrqirx... Mx'w levh xs xlmro sj e qsvi tsaivjyp, piww herkivsyw xssp jsv pmfivxc.[1769]

10.1 SUMMARY OF FINDINGS

This thesis started from the premise that while the "going dark" debate might be overstated by some commentators, encryption has nonetheless the potential of halting or seriously stalling criminal investigations, due to its ever-increasing strength and pervasive nature. By recognizing that privacy (as furthered by encryption) is not an absolute right and that the state has a valid interest in investigating and prosecuting crime, this thesis aimed to propose a framework that could properly balance these opposed values, within an approach that recognizes the unique nature of encryption technology and its dual nature as both inherently beneficial and potentially harmful to society.

Before determining the judicial requirement that such framework requires, the basics underpinnings of encryption technologies were surveyed in Chapter 2, as a way to set the table for the ongoing analysis. In turn, a better understanding of this technology showed that encryption is beneficial for society, except maybe when it is used to hide criminal activities conducted online or to otherwise hide evidence. The chapter also explained why the remainder

[1769] As put by Esther Dyson:

> "Encryption...is a powerful defensive weapon for free people. It offers a technical guarantee of privacy, regardless of who is running the government... It's hard to think of a more powerful, less dangerous tool for liberty."

As cited in Derek Leebaert, ed, *The future of the electronic marketplace*, 2. print ed (Cambridge, Mass.: MIT Press, 1999) at 252 (put through Caesar's famous cipher, using a +4 character equivalence).

of the thesis is free from analogies and comparison (which are usually quite frequent in criminal law and the technological industry), in furtherance of the recognition that encryption is a unique technology, that finds no equivalent in the analog world.

Chapter 3 navigated the idea that encryption reveals a deeper opposition in criminal law between privacy and security, here conceived as the positive result of the state investigating and prosecuting crime. This conflict between values has been the major reason why the "going dark" debate is still at a standstill, many years after its first iteration during the 1990s Crypto wars. This chapter aimed to reconcile privacy and security, in the hopes of resolving this standstill. By properly opposing encryption's positive impacts on privacy and security with the fact that the state is not entitled to the most effective investigative techniques, it is possible to realize that weakening encryption is not a solution to the "going dark" debate.

Chapters 4 and 5 consisted of a deep dive into the applicable *Charter* protections, namely the principle against self-incrimination and the protection against unreasonable search and seizure. Canada's unique experience with both legal concepts provided the necessary basis to subsequently determine if law enforcement should be allowed to compel decryption of data or unlocking of devices by suspects, during the course of an investigation. Specific attention was paid to the applicability of these protections to digital devices and electronic data, particularly when it comes to the protection against unreasonable search and seizure, due to the SCC's long line of decisions on the subject.

In order to provide inspiration as to what a framework regulating encryption could look like in Canada, Chapter 6 examined what has been done on this subject in three countries that share a common judicial heritage with Canada, namely the United States, the United

Kingdom, and Australia. Through the analysis of their different approaches to the subject, what became clear is that very different solutions can be used to address the effects of encryption on criminal investigations, some by way of legislative action, some by judicial interpretation of existing legal principles.

Chapter 7 aimed to harmonize the protections given by ss. 7 and 8 of the *Charter* to create a framework that would be both satisfying from a privacy and a law enforcement perspective. It suggested that compelled decryption of data or unlocking of devices by suspects does not necessarily infringe the *Charter*, if strict conditions are imposed on law enforcement. More specifically, it was suggested that a judicial authorization, available under the standard of *reasonable grounds to believe*, could be crafted to allow such investigative technique only when no other "encryption workaround" is available to law enforcement. In the absence of another "encryption workaround," compelled decryption is the only solution available to law enforcement, making this technique inherently proportional and in accordance with the principles of fundamental justice. *A contrario*, it was submitted that law enforcement should not be granted extraordinary powers, in the absence of extraordinary circumstances.

One of these "encryption workarounds" is the obtention of the relevant evidence from a third party, using a production order. Chapter 8 examined this possibility and strongly advocated against the weakening of encryption, either by way of key escrow mechanisms or backdoors. The chapter suggested that TPDCs could indeed be compelled to hand over data to help law enforcement in its investigations, but not in a manner that would unduly weaken encryption for law abiding citizens and the state alike. The impacts of the delocalization of data on criminal investigations were also examined, including the jurisdictional considerations linked to the remote obtention of data located abroad.

Chapter 9 examined the unique nature of wiretap authorizations and the impact of encryption on the interception of private communications. Building on the idea that strong encryption must remain available due to its inherent benefits, it was suggested that the solution to the "going dark" applied to data in transit can most likely only be found in the use of lawful hacking. As such, Chapter 9 suggested that legislative action should be taken to standardize the use of these techniques and to properly address their potential impacts on international relations, due to their potential transnational application.

10.2 FURTHER THOUGHTS

Encryption of data—at rest and in transit—has become essential and inescapable, in a climate where cybercrime is constantly on the rise[1770] and where individuals and states alike are increasingly relying on electronic communications and digital devices to conduct their activities. Without strong encryption, it is not only individual rights and freedoms that are at risk, but also the structure of the internet itself.[1771] Without strong encryption, events such as the use of Pegasus software against law-abiding citizens[1772] are only going to become more prevalent, as attacks would be extremely easy to conduct for cyber-criminals. The consensus on the necessity of strong encryption is unwavering amongst experts from both the legal domain and the technology industry.

[1770] According to Statistics Canada, total police-reported cybercrime in 2021 augmented from 65,141 cases in 2020 to 70,288 cases in 2021 and has constantly been augmenting since 2014. "Police-reported cybercrime, number of incidents and rate per 100,000 population, Canada, provinces, territories, Census Metropolitan Areas and Canadian Forces Military Police", (2 August 2022), online: *Statistics Canada* <https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=3510000201>.

[1771] Abelson et al, *supra* note 3 at 7.

[1772] See Chapter 9 *supra*.

By definition, encryption aims at ensuring that private information remains private and immune from third party invasion. As such, its use will necessarily frustrate individuals trying to gain access to this private information, whether lawfully or unlawfully. The process of encrypting data is, all things considered, quite straightforward: plain text is transformed into ciphertext,[1773] in the hopes of concealing and protecting the information it contains. While encryption methods have become increasingly sophisticated due to the advent and subsequent evolution of digital technologies, the goal of encryption remains essentially unchanged ever since its first recorded uses, possibly as far back as 1900 BCE.[1774]

In this context, it is unsurprising that encryption has been perceived as both simultaneously beneficial and harmful to society, conversely highlighting the deeper debate found within criminal law about privacy as opposed to security. The "going dark" phenomenon—which postulates that encryption is preventing law enforcement officials from accessing data that is necessary to their investigations[1775]—is the quintessential illustration of the tension between these two interests, which are arguably of equal value. However, by redefining what security means in the context of encryption (and of digital technologies in general), the traditional divide between these seemingly opposed normative preferences can be bridged. The recognition that security in this context also militates towards strong encryption mechanisms will enable lawmakers to find a mutually satisfactory framework for privacy advocates and security proponents alike, especially considering that solutions exist for accessing data in its

[1773] See *inter alia* Solakian, *supra* note 1284 at 221. See also Chapter 2 *supra.*
[1774] Weber, *supra* note 45 at 458–459.
[1775] Comey, *supra* note 3.

decrypted form, without unduly affecting the strength of available encryption for law-abiding citizens.

In addressing the "going dark" debate in its Canadian iteration, this thesis should have made a few key points clear. First, encryption is necessary and important, as a means of promoting individual rights and freedoms globally and of encouraging digital security for any type of entity, from the citizen to the state alike. Any attempt at addressing the "going dark" debate that weakens encryption should not be considered as a sustainable option, as it will inevitably lead to an increase in cyber-attacks, including on governments' highly sensitive data. Second, while encryption has many positive impacts, it does indeed have the potential to hamper law enforcement in their investigations, in turn affecting the state's right and obligation to investigate and prosecute crime. As such, criminal law must attempt to find solutions to this problem, in a manner that adequately balances the opposed interests at play (correctly identified as being privacy on one side, and the state's obligation to investigate and prosecute crime on the other), which is really the keystone of this matter. Third, it must be recognized that the tensions present within the "going dark" debate are deeply influenced by social narratives that are inherently unpredictable. On one side, events such as the 9/11 terrorist attacks or the San Bernardino shootings bring "crime control"[1776] values to the forefront, while on the other side revelations of mass surveillance conducted by governments[1777] amplify privacy concerns and promote "due process"[1778] values. Supporters of each approach

[1776] To use Packer's now famous dichotomous terminology. Packer, *supra* note 292.
[1777] Liguori, *supra* note 70 at 323; Lear, *supra* note 72; Taylor, *supra* note 3 at 217.
[1778] Packer, *supra* note 292.

use these events to further their own positions, demonstrating that normative preferences highly influence policy choices.

In this context, Canadian criminal law is at a crossroads where it must decide how to resolve this problematic, by either adapting its current laws or by recognizing the unique nature of encryption technologies and creating a new approach via legislation. While the SCC and the Canadian Parliament have not necessarily followed a clear approach towards the regulation of technologies throughout the years,[1779] this thesis has hinted at the possibility that the adoption of an overarching model could create a more coherent framework in the long run.

By recognizing that encryption has no functional or historical equivalent, this thesis proposed a compelled decryption framework that uniquely considers the links between the protection against self-incrimination found in s. 7 of the *Canadian Charter of Rights and Freedoms*[1780] and the protection against unreasonable search and seizure found in s. 8. The interplay between these protections has not always been clear, even within the SCC's jurisprudence. By focusing on the reasonableness aspect found in ss. 7 and 8 of the *Charter*, it has been suggested that a compelled decryption framework that respects the imperatives inherent in these provisions, can be created, in a manner that is proactive, coherent, balanced, and adaptable.

The suggested framework recognizes the unique nature of the Canadian approach to self-incrimination, which favors the search for truth by way of testimonial immunities, rather than a general right to refuse to answer questions. The framework also acknowledges the emphasis

[1779] Aylward, *supra* note 655.
[1780] *Charter*, *supra* note 24.

that Canadian criminal law has placed on the importance of right to remain silent and the general distaste it has for self-incrimination. Accordingly, the framework suggests that immunities need to be granted to suspects regarding the act of decryption and that compelled decryption should only be available following the obtention of a judicial authorization, in settings where no other "encryption workaround"[1781] is reasonably applicable. This effectively recognizes that in circumstances where law enforcement is not stalled by encryption, it should not be given a power to compel decryption, due to the strength of privacy and self-incrimination interests at play.

Importantly, the proposed framework recognizes that alphanumeric passcodes and biometric authentication measures are functionally equivalent and should receive the same protection, which effectively casts aside an illusory distinction that is not supported by the technology itself or the overarching goals of ss. 7 and 8. This has the advantage of allowing individuals to use biometric authentication methods, which are more secure than alphanumeric passcodes,[1782] without running the risk of receiving lesser protection. Consequentially, this also avoids a potential exodus toward alphanumeric passcodes, as a reaction to the lesser judicial protections biometric authentication measures would otherwise receive.

To be clear, the compelled decryption framework suggested in Chapter 7 might become obsolete if lawful hacking indeed gets recognized as the best investigative technique to circumvent encryption. The self-incrimination and privacy impacts of compelled decryption are not to be casually cast aside. Rather, it is only when other alternatives are not reasonably

[1781] Kerr & Schneier, *supra* note 22.
[1782] Herrera, *supra* note 212 at 786; Vayas, *supra* note 1475 at 1647; Phelps, *supra* note 1313 at 464; Sherman, *supra* note 217 at 666.

applicable that compelled decryption should be authorized by a court. As such, if lawful hacking provisions are adopted and more funding is given to law enforcement agencies to implement the use of lawful hacking, compelled decryption might rapidly become futile, except in situations where officers are not able to gain access to a device, either because of the absence of a security weakness in the targeted device or software, or because "social engineering" techniques have failed.

Lawful hacking is not only a potential solution to the encryption of data at rest, but also of data in transit. As the "going dark" problem expands to encrypted electronic communications, due to the rise of E2EE and perfect forward secrecy, the use of techniques usually employed by hackers is promising to level the field and ensure continuing access to intercepted communications *en clair* for law enforcement. As with the proposal for compelled decryption framework as a solution to the encryption of data at rest, this has the benefit of allowing strong encryption to remain available to all, while providing an alternative to law enforcement.

Lessons from other jurisdictions, such as the United States, Australia, and the United Kingdom, show that compelled decryption is increasingly perceived as a viable solution to the "going dark" debate, especially when combined with lawful hacking provisions. While these countries' experiences with self-incrimination and unreasonable searches and seizures are undeniably different from Canada's, the unique path they have all decided to follow provides an interesting starting point for Parliament to regulate compelled decryption and lawful hacking in Canada. Generally speaking, lessons from these countries show that compelled decryption and lawful hacking are two methods that are complementary when it comes to attempting to find a solution to the "going dark" problem.

Yet, lawful hacking uniquely challenges the traditional idea that a country's enforcement jurisdiction cannot be exercised extraterritorially, in a way that highlights the need for international rules on comity and sovereignty to evolve in light of digital technologies and the ubiquitous nature of the internet. While the jurisdictional issues linked to electronic searches are not unique to encrypted communications and data, lawful hacking defies territorial boundaries in a way that is novel, due to the fact that law enforcement could—knowingly or unknowingly—be encroaching on another state's sovereignty. While these considerations have only been touched upon in this thesis and further analysis on this subject is necessary and important, it seems that a movement towards allowing states to remotely access data located outside their borders, without it being considered an intrusion into another country's sovereign territory, is rapidly gaining traction on the international scene.

The intersection of criminal law and technology is always in flux, prompting the need for malleable and adaptable law enforcement investigative powers that can grow with new technologies. The combined approach to the encryption problem found within the suggested compelled decryption framework and the use of lawful hacking techniques is necessarily subject to the same need. Recent discoveries in the area of quantum computing might provide an additional solution to the "going dark" problem, because of the incredible decrypting capacities that such computers would have.[1783] Regardless, the creation of such machines is still uncertain and could only happen in a very distant future, justifying a revised and concerted Canadian approach to encrypted evidence in the meantime. This thesis has aimed to do exactly that, by providing a dual solution to the "going dark" problem, found within

[1783] Amit Katwala, "Quantum computers will change the world (if they work)" *Wired* (5 March 2020), online: <https://www.wired.co.uk/article/quantum-computing-explained>.

investigative techniques that are aptly suited to the unique nature of encryption and the impact it has on individual rights and freedoms.

BIBLIOGRAPHY

Canadian Legislation

An Act respecting national security matters, 1st Sess, 42nd Parl, 2019 (assented to 21 June 2019), SC 2019, c 13.

Canada Evidence Act, LRC 1985, c C-5, s 4.

Canadian Bill of Rights, SC 1960, c 44.

Criminal Code, RSC 1985, c C-46.

Canadian Charter of Rights and Freedoms, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK).

Combines Investigation Act, RSC 1970, c C-23.

Competition Act, RSC 1985, c C-34.

DNA Identification Act, 1998.

Identification of Criminals Act, RSC 1985, c I-1.

Interpretation Act, RSC 1985, C I-21, s 34.

Mutual Legal Assistance in Criminal Matters Act, RSC 1985, c 30 (4th supp).

Personal Information Protection and Electronic Documents Act, SC 2000, c 5.

Protecting Canadians from Online Crime Act, SC 2014, c 31.

International Legislation

Australia, *Crimes Act 1914*, No 12 (1914).

Australia, *Privacy Act 1988*, No 119 (1988).

Australia, *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, No 148 (2018).

Council of Europe, *Convention on Cybercrime*, (ETS No 185), Budapest, 23 November 2001.

Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos 11 and 14*, 4 November 1950, ETS 5.

Council of Europe, *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, CETS No 224, 2022.

European Parliament, *Charter of Fundamental Rights of the European Union*, C 326/391 (2012).

New South Wales Government, *Law Enforcement (Powers and Responsibilities) Act 2002*.

Queensland Government, *Police Powers and Responsibilities Act 2000*, No 103 (2000).

United Kingdom, *Investigatory Powers Act 2016*, c 25, 2016.

United Kingdom, *Regulation of Investigatory Powers Act 2000*, c 23, 2000.

United Kingdom, *Police and Criminal Evidence Act 1984*, UK Public General Acts, s 66, 1984.

United Nations General Assembly, *International Covenant on Civil and Political Rights*, (16 December 1966).

United Nations General Assembly, *Universal Declaration of Human Rights*, (10 December 1948).

United States, *All Writs Act*, 28 USC 1651.

United States, *Communications Assistance for Law Enforcement Act*, 47 USC (2018).

United States, 116th Congress, *Lawful Access to Encrypted Data Act*, s 4051 (2019-2020).

United States, 115th Congress, *Clarifying Lawful Overseas Use of Data (CLOUD) Act*, HR 4943, 2018.

Victoria Legislation, *Crimes Act 1958*.

Canadian Jurisprudence

A c R, 2021 QCCS 5440.

Application for a General Warrant Pursuant to s 487.01 Cr. C. (Re), [2008] CanLII 85918.

Application for production order (Re), 2020 NSPC 55.

Application under s 83.28 of the Criminal Code (Re), 2004 SCC 43, [2004] 2 SCR 248.

B (R) v Children's Aid Society of Metropolitan Toronto, [1995] 1 SCR 315.

Blencoe v British Columbia (Human Rights Commission), 2000 SCC 44, [2000] 2 SCR 307.

British Columbia (Attorney General) v Brecknell, 2018 BCCA 5.

British Columbia Securities Commission v Branch, [1995] 2 SCR 3.

Canada (Attorney General) v Bedford, 2013 SCC 72, [2013] 3 SCR 1101.

Canadian Foundation for Children, Youth and the Law v Canada (Attorney General), 2004 SCC 76, [2004] 1 SCR 76.

Canadian Security Intelligence Service Act (Can) (Re), 2019 FC 141, [2019] 2 FCR 359.

CanadianOxy Chemicals Ltd v Canada (Attorney General), [1999] 1 SCR 743.

Cloutier v Langlois, [1990] 1 SCR 158.

Curr v R, [1972] SCR 889.

Dagenais v Canadian Broadcasting Corp, [1994] 3 SCR 835.

Dedman v The Queen, [1985] 2 SCR 2.

Dersch v Canada (Attorney General), [1990] 2 SCR 1505.

Dubois v The Queen, [1985] 2 SCR 350.

Fleming v Ontario, 2019 SCC 45; [2019] 3 SCR 519.

Google Inc v Equustek Solutions Inc, 2017 SCC 34, [2017] 1 SCR 824.

Hunter v Southam Inc, [1984] 2 SCR 145.

Impression Warrant Application (Re), 2016 ONCJ 197.

In the Matter of a Reference Pursuant to Section 27(1) of the Judicature act, Chapter J-1 of the Revised Statutes of Alberta, 1980, as amended, referred by Order in Council (OC 84/83) of the Lieutenant Governor in Council dated the 2nd day of February, AD 1983, to the Court of Appeal of Alberta, [1984] 2 SCR 697.

In the matter of an application to obtain a production order pursuant to section 487014 of the Criminal Code of Canada, 2018 NLPC 2369.

Irwin Toy Ltd v Quebec (Attorney General), [1989] 1 SCR 927.

Marcoux and Solomon v R, [1976] 1 SCR 763.

Morgentaler v R, [1988] 1 SCR 30.

O'Reilly c R, 2017 QCCA 1283.

Re BC Motor Vehicle Act, [1985] 2 SCR 486 at 519.

R c Bissonnette, 2020 QCCS 845.

R c Boudreau-Fontaine, 2010 QCCA 1108.

R c Faivre, 2018 QCCQ 7467.

R c McGown, 2016 ONCA 575.

R c Mirarchi, 2015 QCCS 6628.

R c Mirarchi, 2015 QCCS 6629.

R v Adem, 2021 ONCJ 210.

R v Amer, 2017 ABQB 651.

R v Amway Corp, [1989] 1 SCR 21.

R v Araujo, 2000 SCC 65, [2000] 2 SCR 992.

R v Aucoin, 2012 SCC 66, [2012] 3 SCR 408.

R v Azonwanna, 2020 ONSC 5416.

R v Battista et al, 2011 ONSC 4771.

R v Beare, [1988] 2 SCR 387.

R v Beauchamp, [2009] CanLII 64185.

R v BH, 2020 ONSC 4533.

R v Big M Drug Mart, [1985] 1 SCR 295.

R v Bishop, 2002 NSPC 2.

R v Bishop, 2007 ONCJ 441.

R v Bishop, 2013 BCSC 522.

R v Boersma, [1994] 2 SCR 488.

R v Borden, [1994] 3 SCR 145.

R v Boutros, 2018 ONCA 375.

R v Brewster, 2016 ONSC 4133.

R v Brown, 2002 SCC 32, [2002] 2 SCR 185.

R v Brown, 2022 CSC 18

R v Buhay, 2003 SCC 30, [2003] 1 SCR 631.

R v Burke, 2013 ONCA 424.

R v Burke, 2015 SKPC 173.

R v Buss, 2014 BCPC 16.

R v Capancioni, 2016 ONSC 4615.

R v Caslake, [1998] 1 SCR 51.

R v CCM, 2012 MBQB 141.

R v Chen, 2017 ONSC 4083.

R v Clayton, 2007 SCC 32, [2007] 2 SCR 725.

R v Cody, [2013] CanLII 94260.

R v Colarusso, [1994] 1 SCR 20.

R v Cole, 2012 SCC 53, [2012] 3 SCR 34.

R v Collins, [1987] 1 SCR 265.

R v Commisso, [1983] 2 SCR 121.

R v Connors, [1998] CanLII 12468.

R v Cornell, 2010 SCC 31, [2010] 2 SCR 142.

R v Côté, 2011 SCC 46, [2011] 3 SCR 215.

R v Crawley, 2018 ONCJ 394.

R v Cuthill, 2016 ABQB 60.

R v Darrach, 2000 SCC 46, [2000] 2 SCR 443.

R v Debot, [1989] 2 SCR 1140.

R v Dersch, [1993] 3 SCR 768.

R v Do, 2002 BCSC 1889.

R v DO, 2021 BCPC 171.

R v Duarte, [1990] 1 SCR 30.

R v Dyment, [1988] 2 SCR 417.

R v Edwards, [1996] 1 SCR 128.

R v El-Halfawi, 2021 ONCJ 462.

R v Evans, [1991] 1 SCR 869.

R v Evans, [1996] 1 SCR 8.

R v Fearon, 2014 SCC 77, [2014] 3 SCR 621.

R v Ferguson, 2018 BCSC 594.

R v Finlay, [1985] 23 SCC (3d) 48.

R v Finlay, [1993] 3 SCR 103.

R v Fitzpatrick, [1995] 4 SCR 154.

R v Ford, [2017] QSC 205.

R v G (B), [1999] 2 SCR 475.

R v Garofoli, [1990] 2 SCR 1421.

R v Giles, 2007 BCSC 1147.

R v Godoy, [1999] 1 SCR 311.

R v Golden, 2001 SCC 83, [2001] 3 SCR 679.

R v Gomboc, 2010 SCC 55, [2010] 3 SCR 211.

R v Grant, [1993] 3 SCR 223.

R v Grant, 2009 SCC 32, [2009] 2 SCR 353.

R v Ha, 2009 ONCA 340.

R v Handy, 2002 SCC 56, [2002] 2 SCR 908.

R v Hape, 2002 SCC 26, [2007] 2 SCR 292.

R v Harder, 2017 ONCJ 280.

R v Hart, 2014 SCC 52, [2014] 2 SCR 544.

R v Hart, 2015 ONCJ 831.

R v Hebert, [1990] 2 SCR 151.

R v Henry, 2005 SCC 37, [2005] 3 SCR 609.

R v H-G (R), 2005 QCCA 1160.

R v Hiscock, [2016] CanLII 96899.

R v Hodgson, [1998] 2 SCR 449.

R v Hundal, [1993] 1 SCR 867.

R v H (TG), 2014 ONCA 460.

R v Jarvis, 2002 SCC 72, [2002] 3 SCR 757.

R v Jarvis, 2002 SCC 10, [2019] SCR 10.

R v Jennings, 2018 ABQB 296.

R v JJ, 2022 CSC 28.

R v Jobin, [1995] 2 SCR 78.

R v Johnson, 2021 ONSC 1307.

R v Jones, [1994] 2 SCR 229.

R v Jones, 2011 ONCA 632.

R v Jones, 2017 SCC 60, [2017] 2 SCR 696.

R v Jones, 2019 ONCJ 805.

R v Jordan, 2016 SCC 27, [2016] 1 SCR 631.

R v Kang-Brown, 2008 SCC 18, [2008] 1 SCR 456.

R v Kossick, 2018 SKCA 55.

R v Kuitenen, 2001 BCSC 677.

R v Kuldip, [1990] 3 SCR 618.

R v KZ, 2014 ABQB 235.

R v Larsen, 2011 SKPC 195.

R c Lauzon, 2019 ONCA 546.

R v Le, 2019 SCC 34, [2019] 2 SCR 692.

R v Love, 2022 ABCA 269.

R v Lucas, [2009] CanLII 43423.

R v Lyons, [1987] 2 SCR 309.

R v Mabior, 2012 SCC 47, [2012] 2 SCR 584.

R v MacDonald, 2014 SCC 3, [2014] 1 SCR 37.

R v Mann, 2004 SCC 52, [2004] 3 SCR 59.

R v Mannion, [1986] 2 SCR 272.

R v Marakah, 2017 SCC 59, [2017] 2 SCR 608.

R v McBride, 2017 BCSC 1016.

R v Merritt, 2017 ONSC 5245.

R v Millard and Smich, 2016 ONSC 348.

R v Mills, [1999] 3 SCR 668.

R v Mills, 2019 SCC 22, [2019] 2 SCR 320.

R v Morelli, 2010 SCC 8, [2010] 1 SCR 253.

R v Navia, 2020 ABPC 20.

R v Nedelcu, 2012 SCC 59, [2012] 3 SCR 311.

R v Nero, 2016 ONCA 153.

R v Nguyen, 2013 BCSC 950.

R v Nicholson, [1999] CanLII 6728.

R v Noble, [1997] 1 SCR 874.

R v Noël, 2002 SCC 67, [2002] 3 SCR 433.

R v Nolet, 2010 SCC 24, [2010] 1 SCR 851.

R v Oakes, [1986] 1 SCR 103.

R v O'Connor, [1995] 4 SCR 411.

R v Oickle, 2010 SCC 38, [2000] 2 SCR 3.

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

R v Otto, 2019 ONSC 2473.

R v Owen, 2017 ONCJ 729.

R v P (MB), [1994] 1 SCR 555.

R v Partanen, 2021 BCPC 245.

R v Patrick, 2009 SCC 17, [2009] 1 SCR 579.

R v Pelich, 2012 ONSC 3611.

R v Pelucco, 2013 BCSC 588.

R v Petrin, 2016 ABQB 375.

R v Plant, [1993] 3 SCR 281.

R v Playford, [1987] CCC (3d) 142.

R v Pratchett, 2016 SKPC 19.

R v Primeau, [1995] 2 SCR 60.

R v Quesnelles, 2014 SCC 46, [2014] 2 SCR 390.

R v Reeves, 2018 SCC 56, [2018] 3 SCR 531.

R v Rodgers, 2006 SCR 15, [2006] 1 SCR 554.

R v Rose, [1998] 3 SCR 262.

R v S (RJ), [1995] 1 SCR 451.

R v SAB, 2003 SCC 60, [2003] 2 SCR 678.

R v Saeed, 2016 SCC 24, [2016] 1 SCR 518.

R v Sawatsky, [1997] CanLII 511.

R v SE, 2021 ONSC 4124.

R v Seaboyer; R c Gayme, [1991] 2 SCR 577.

R v Seguin, 2015 ONSC 1908.

R v Shergill, 2019 ONCJ 54.

R v Silveira, [1995] 2 SCR 297.

R v Simmons, [1988] 2 SCR 495.

R v Singh, 2007 SCC 48, [2007] 3 SCR 405.

R v SL, 2019 ONCJ 101.

R v Smith, Wynter, 2017 ONSC 4683.

R v Sonne, 2012 ONSC 2126.

R v Spencer, 2014 SCC 43, [2014] 2 SCR 212.

R v Stack, 2021 ONCJ 274.

R v Stairs, 2022 SCC 11.

R v Stemberger, 2012 ONCJ 31.

R v Stillman, [1997] 1 SCR 607.

R v Stinchcombe, [1991] 3 SCR 326.

R v Strong, 2020 ONSC 7528.

R v Suberu, 2009 SCC 33, [2009] 2 SCR 460.

R v Subia, 2021 ONSC 6628.

R v Suter, 2018 SCC 34, [2018] 2 SCR 496.

R v Talbot, 2017 ONCJ 814.

R v Tang, 2009 ONCJ 642.

R v Taylor, 2014 SCC 50, [2014] SCR 495.

R v TELUS Communications Co, 2013 SCC 16, [2013] 2 SCR 3.

R v Tessling, 2004 SCC 67, [2004] 3 SCR 341.

R v Therens, [1985] 1 SCR 613.

R v Thompson, [1990] 2 SCR 1111.

R v Thompson, 2001 CanLII 24186 (ON CA).

R v Tim, 2022 SCC 12.

R v Tse, 2012 SCC 16, [2012] 1 SCR 531.

R v Tsekouras, 2012 ONSC 5137.

R v Turcotte, 2005 SCC 50, [2005] 2 SCR 519.

R v Twitchell, 2010 ABQB 693.

R v Underwood, [1998] 1 SCR 77.

R v Villaroman, 2012 ABQB 630.

R v VI, 2008 CanLII 36164 (ON SC).

R v VL, 2011 ONSC 218.

R v Vu, 2013 SCC 60, [2013] 3 SCR 657.

R v Weir, 2001 ABCA 181.

R v White, [1999] 2 SCR 417.

R v Whittle, [1994] 2 SCR 914.

R v Wiggins, [1990] 1 SCR 61.

R v Wiley, [1993] 3 SCR 263.

R v Williams, 2014 NBJ 356.

R v Winchester, 2010 ONSC 652.

R v Wong, [1990] 3 SCR 36.

R v Wong, 2017 BCSC 306.

Re Application for a Production Order, s. 487.014 of the Criminal Code, 2019 ONCJ 775.

Re Subscriber Information, 2015 ABPC 178.

Rothman v R, [1981] 1 SCR 640.

RWDSU v Dolphin Delivery Ltd, [1986] 2 SCR 573.

SPVM c JPM, unreported decision [500-36-009870-216, 500-26-123252-219] (QCCS).

Thomson Newspapers Ltd v Canada, [1990] 1 SCR 425.

Uber Canada inc c Agence du revenu du Québec, 2016 QCCS 2158.

United State v Equinix Inc, 2017 ONCA 260.

Williams c R, 2018 NBCA 70.

Wu c R, 2019 QCCA 1702.

X (Re), 2017 FC 1047.

International Jurisprudence

Barrera, [2019] WL 6253812.

Blau v United States, 340 US 159 (1950).

Boyd v United States, 1886 US 616.

Carpenter v United States, 138 S Ct 2206 (2018).

Commonwealth v Baust, 89 Va Cir 267 (2014).

Commonwealth v Gelfgatt, 11 NE3d 605 (2014).

Doe v United States, 487 US 201 (1988).

Fisher v United States, 425 US 391 (1976).

Greater Manchester Police v Andrews, [2011] EWHC 1966.

Hoffman v United States, 341 US 479 (1951).

In Re Application for a Search Warrant, 236 F Supp 3d 1066 (2017).

In Re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F3d 1335 (2012).

In re Grand Jury Subpoena to Boucher, 2009 WL 424718.

In Re Search of a White Google Pixel 3XL Cellphone in a Black Incipro Case, 398 F Supp 3d 785 (2019).

In re Search of Residence in Oakland, CA, 354 F Supp 3d 1010 (2019).

In re The Decryption of a Seized Data Storage System (Feldman), 2013 US Dist LEXIS 202353.

Kastigar v United States, 406 US 441 (1972).

Katz v United States, 1967 US 347.

Lee v New South Wales Crime Commission, 302 ALR 363.

Lee v The Queen, [2014] HCA 20.

Pennsylvania v Muniz, 496 US 582 (1990).

Matter of Search Warrant Application for [redacted text], 2017 WL 4563861.

Matter of Single-family Home & Attached Garage, 2017 WL 4563870.

Miranda v Arizona, 384 US 436 (1966).

Riley v California, 575 US 373 (2014)

R v S(F), 1 WLR 1489 (2009).

R v Waterfield, 1963 All ER 659.

Saunders v United Kingdom, 23 Eur HR Rep 313 (1996).

Schmerber v California, 384 US 757 (1966).

SEC v Huang, 2015 WL 5611644.

Semayne's Case (1604), 5 Co Rep 91, 77 ER 194.

Seo v State, 109 NE 3d 418 (2018).

Sorby v The Commonwealth, [1983] 152 CLR 281.

State v Diamond, 890 NW2d 143 (2017).

State v Stahl, 206 So 3d 124 (2016).

United States v Apple MacPro Computer, 851 F3d 238 (2017).

United States v Fricosu, 841 F Supp 2d 1232 (2012).

United States v Hubbell, 30 US 27 (2000).

United States v Kirschner, 823 F Supp 2d 665 (2010).

United States v Pearson, [2006] US Dist LEXIS 32982.

United States v Scarfo, 180 F Supp 2d 572 (2001).

United States v Wright, 2020 WL 60239.

US v Sealed Warrant, 2019 WL 4047615.

Secondary Materials: Monographs

Béliveau, Pierre & Martin Vauclair, *Traité général de preuve et de procédure pénales* ([Montréal]; Cowansville: Éditions Thémis ; Éditions Yvon Blais, 2013).

Bentham, Jeremy, "An Introduction to the Principle of Morals and Legislation" in JH Burns & HLA Hart, eds, (London: Methuen, 1970).

———, "Principles of Judicial Procedure with the Outlines of a Procedure Code" in John Bowring, ed, *Works Jeremy Bentham* (Edinburgh: William Tait, 1843).

———, "On Exclusion of Evidence" in John Bowring, ed. *Works of Jeremy Bentham* (Edinburgh: William Tait, 1843).

Coughlan, Steve, *Criminal procedure*, fourth edition ed, Essentials of Canadian law (Toronto: Irwin Law, 2020).

Currie, Robert J & Joseph Rikhof, *International & transnational criminal law*, third edition ed, Essentials of Canadian law (Toronto, ON: Irwin Law, 2020).

Dooley, John F, *History of Cryptography and Cryptanalysis: Codes, Ciphers, and Their Algorithms*, History of Computing (Cham, Switzerland: Springer, 2018).

Farmer, Lindsay, *Making the modern criminal law: criminalization and civil order*, first edition ed (Oxford, United Kingdom: Oxford University Press, 2016).

Geist, Michael, ed, *Law, privacy and surveillance in Canada in the post-Snowden era*, Law, technology and media (Ottawa, Ontario: University of Ottawa Press, 2015).

Gerlach, Neil, *The genetic imaginary: DNA in the Canadian criminal justice system*, Digital futures (Toronto; Buffalo: University of Toronto Press, 2004).

Hadnagy, Christopher, *Social engineering: the art of human hacking* (Indianapolis, IN: Wiley, 2011).

Hobbes, Thomas, *Leviathan: Or the Matter, Forme and Power of a Commonwealth Ecclesiasticall and Civil* (1651).

Hubbard, Robert W, Peter M Brauti & Scott K Fenton, *Wiretapping and other electronic surveillance: law and procedure* (Toronto: Canada Law Book, Thomson Reuters Canada, 2022).

Iftene, Adelina, "Mr. Big: The Undercover Breach of the Right against Self-Incrimination" in Chris Hunt, ed., *Perspective on Evidentiary Privileges* (Toronto: Carswell, 2019).

Inness, Julie, *Privacy, Intimacy, and Isolation* (New York: Oxford University Press, 1992).

Jarvis, Craig, *Crypto wars: the fight for privacy in the digital age: a political history of digital encryption* (Boca Raton London New York: CRC Press / Taylor & Francis Group, 2021).

Koops, Bert-Jaap & Susan W Brenner, eds, *Cybercrime and jurisdiction: a global survey*, Information technology & law series 11 (The Hague : West Nyack, NY: TMC Asser ; Cambridge University Press [distributor], 2006).

Levy, Leonard W, *Origins of the Fifth Amendment: The Right Against Self-Incrimination* (Oxford: Oxford University Press, 1968).

Locke, John, *Second Treatise of Government* (Awnsham Churchill, 1689).

Molitorisz, Sacha, *Net privacy: how we can be free in an age of surveillance* (Montreal: McGill University Press, 2020).

Moore, Adam D, *Privacy Rights - Moral and Legal Foundations* (University Park, Pennsylvania: The Pennsylvania State University Press, 2010).

National Academies of Sciences, Engineering, and Medicine (US), ed, *Decrypting the encryption debate: a framework for decision makers*, Consensus study report (Washington, DC: The National Academies Press, 2018).

Nissenbaum, Helen Fay, *Privacy in context: technology, policy, and the integrity of social life* (Stanford, California: Stanford Law Books, 2010).

Paciocco, David M & Lee Stuesser, *The Law of Evidence*, 5th ed (Toronto: Irwin Law, 2010).

Rousseau, Jean-Jacques, *Du Contrat Social, ou Principes du Droit Politique* (1762).

Watt, David, *Law of electronic surveillance in Canada*, Carswell's criminal law series (Toronto: Carswell, 1979).

Westin, Alan F, *Privacy and Freedom* (New York: Atheneum, 1967).

Wigmore, John Henry, *Principles of judicial proof, as given by logic, psychology, and general experience, and illustrated in judicial trials* (Boston: Little, 1913).

Our Security, Our Rights National Security Green Paper, 2016. (Ottawa, Canada: Public Safety Canada, 2016).

Secondary Materials: Articles

Abraha, Halefom H, "Regulating law enforcement access to electronic evidence across borders: The United States approach" (2020) 29:3 Information & Communications Technology Law 324.

Adra, Bilal, "Facing the Facts on Biometric Phone Locks: Your Face and Thumb Are Not Secure" (2018) 2018:2 University of Illinois Journal of Law, Technology & Policy 407.

Ahlam, Rafita, “Apple, the Government, and You: Security and Privacy Implications of the Global Encryption Debate” (2021) 44:3 Fordham International Law Journal 771.

Ajello, Nicholas J, “Fitting a Square Peg in a Round Hole: Bitcoin, Money Laundering, and the Fifth Amendment Privilege against Self-Incrimination” (2015) 80:2 Brooklyn Law Review 435.

Alschuler, Albert W, “A Peculiar Privilege in Historical Perspective: The Right to Remain Silent” (1995) 94 Michigan Law Review 2625.

Anderson, Heidi R, “The Mythical Right to Obscurity: A Pragmatic Defense of No Privacy in Public” (2012) 7 I/S: Journal of Law and Policy for the Information Society 543.

Arenella, Peter, “Rethinking the Functions of Criminal Procedure: The Warren and Burger Courts’ Competing Ideologies” (1983) 72 Georgetown Law Journal 185.

Atrens, Jerome, “A Comparison of Canadian and American Constitutional Law Relating to Search and Seizure” (1994) 1 Southwest Journal of Law & Trade in the Americas 29–48.

Atwood, J Riley, “The Encryption Problem: Why the Courts and Technology Are Creating a Mess for Law Enforcement” (2015) 34 St Louis University Public Law Review 407.

Aucoin, Kaleigh E, “The Spider’s Parlor: Government Malware on the Dark Web” (2018) 69:5 Hastings Law Journal 1433.

Austin, Lisa M, “Towards a Public Law of Privacy: Meeting the Big Data Challenge” (2015) 71:2 Supreme Court Law Review (2d) 541.

Aylward, Stephen, “Technological Neutrality or Novelty? Two Models of Privacy in the Digital Era” (2017) 80 Supreme Court Law Review (2d) 423.

Babiarz, Christopher, “Encryption Friction” (2017) 10 Albany Governmental Law Review 351.

Bailey, Abe Andrew, “Privacy, Privilege, and Protection: A Case for Fifth Amendment Expansion” (2019) 29:2 University of Florida Journal of Law and Public Policy 167.

Bales, Chase, “Unbreakable: The Fifth Amendment and Computer Passwords” (2012) 44 Arizona State Law Journal 1293.

Bambauer, Derek E, “Privacy versus Security” (2013) 103:3 Journal of Criminal Law and Criminology 667.

Bandes, Susan A, “Protecting the Innocent as the Primary Value of the Criminal Justice System” (2009) 7 Ohio State Journal of Criminal Law 413.

Barton, Joe, “Reforming the Mutual Legal Assistance Treaty Framework to Protect the Future of the Internet” (2018) 79 Ohio State Law Journal Furthermore 91.

Beller, Cambrea, “Unlocking Your Phone Could Lock you up: Say Your Goodbyes to the Right against Self-Incrimination” (2020) 55:1 New England Law Review 27.

Bellovin, Steven M et al, “Seeking the Source: Criminal Defendants’ Constitutional Right to Source Code” (2021) 17:1 Ohio State Technology Law Journal 1.

Bellovin, Steven M, Matt Blaze & Susan Landau, “Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet” (2014) 12:1–2 Northwest Journal of Technology and Intellectual Property 1.

Bercovitz, Rachel, “Law Enforcement Hacking: Defining Jurisdiction” (2021) 121:4 Columbia Law Review 1251.

Berger, Mark, “Europeanizing Self-Incrimination: The Right to Remain Silent in the European Court of Human Rights” (2006) 12:2 Columbia Journal of European Law 339.

———, “Reforming Confession Law British Style: A Decade of Experience with Adverse Inferences from Silence” (2000) 31:2 Columbia Human Rights Law Review 243.

———, “Rethinking Self-Incrimination in Great Britain” (1984) 61:3 Denver Law Review 507.

Bilgic, Secil, “Something Old, Something New, and Something Moot: The Privacy Crisis Under the CLOUD Act” (2018) 32:1 Harvard Journal of Law and Technology 321.

Blair, Chris, “Miranda and the Right to Silence in England” (2003) 11:1 Tulsa Journal of Comparative and International Law 1.

Blanch, Joey L & Stephanie S Christensen, “Biometric Basics: Options to Gather Data from Digital Devices Locked by Biometric Key” (2018) 66 US Attorney’s Bulletin 3.

Bonin, Adam C, “Protecting Protections: First and Fifth Amendment Challenges to Cryptography Regulation” (1996) University of Chicago Legal Forum 495.

Bradford Franklin, Sharon, “The Need for Countries to Establish Robust and Transparent Vulnerabilities Equities Processes” (2019) 6:1 Fletcher Security Review 45.

Bradshaw, Simon, Christopher Millard & Ian Walden, “Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services” (2011) 19:3 International Journal of Law and Information Technology 187.

Bratman, Benjamin E, “Brandeis and Warren’s the Right to Privacy and the Birth of the Right to Privacy” (2001) 69 Tennessee Law Review 623.

Brejt, Raila Cinda, “Abridging the Fifth Amendment: Compelled Decryption, Passwords, & Biometrics” (2021) 31:4 Fordham Intellectual Property, Media & Entertainment Law Journal 1154.

Brenner, Susan W, "Encryption, Smart Phones, and the Fifth Amendment" (2012) 33 Whittier Law Review 525.

———, "Law, Dissonance, and Remote Computer Searches" (2012) 24:1 N C J Law Technol 43–92.

———, "The Fifth Amendment, Cell Phones and Search Incident: A Response to Password Protected" (2010) 96 Iowa Law Review Bulletin 78.

Brill, Hillary & Scott Jones, "Little Things and Big Challenges: Information Privacy and the Internet of Things" (2017) 66 American University Law Review 1183.

Brown, Darryl K, "Criminal Law Theory and Criminal Justice Practice" (2012) 49 American Criminal Law Review 73.

Buggie, Chelsey, "Talking to Strangers: A Critical Analysis of the Supreme Court of Canada's Decision in *R v Mills*" (2021) 44:5 Manitoba Law Journal 108.

Cahill, Michael T, "Retributive Justice in the Real World" (2007) 85 Washington University Law Review 815.

Calarco, Paul, "*R v Nedelcu*: Whatever Happened to a Large and Liberal Interpretation of *Charter* Rights?" (2012) 96 CR (6th) 438.

Capisizu, Larisa-Antonia, "Legal Perspectives on the Internet of Things" (2018) Conferinta Internationala de Drept, Studii Europene si Relatii Internationale 523.

Cauthen, Robert H, "The Fifth Amendment and Compelling Unencrypted Data, Encryption Codes, and Passwords" (2017) 41 American Journal of Trial Advocacy 119.

Chan, Gerald, "Text Message Privacy: Who Else Is Reading This?" (2019) 88 Supreme Court Law Review (2d) 69.

Chan, Gerald & Stephen Aylward, "FBI v. Apple and beyond: Encryption in the Canadian Law of Digital Search and Seizure" (2016) 1:1 Journal of Data Protection & Privacy 2.

Chen, Christine W, "The Graymail Problem Anew in a World Going Dark: Balancing the Interests of the Government and Defendants in Prosecutions Using Network Investigative Techniques (NITs)" (2017) 19:1 Columbia Science & Technology Law Review 185.

Choi, Bryan H, "For Whom the Data Tolls: A Reunified Theory of Fourth and Fifth Amendment Jurisprudence" (2015) 37 Cardozo Law Review 185.

———, "The Privilege against Cellphone Incrimination" (2018) 97 Texas Law Review Online 73.

Christianson, Adriana, “Locked out or Locked up: The Need for New Guidelines for Compelled Decryption” (2022) 55:2 Suffolk University Law Review 237.

Clarke, Roger, “Privacy Impact Assessment in Australian Contexts” (2008) 15 eLaw Journal 72.

Cockfield, Arthur J, “Protecting the Social Value of Privacy in the Context of State Investigations Using New Technologies” (2007) 40 University of British Columbia Law Review 41.

Cohen, Aloni & Sunoo Park, “Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries” (2018) 32:1 Harvard Journal of Law & Technology 169.

Colangelo, Alex & 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 McGill Law Journal 47.

Colarusso, David, “Heads in the Cloud, a Coming Storm - The Interplay of Cloud Computing, Encryption, and the Fifth Amendment’s Protection against Self-Incrimination” (2011) 17 Boston University Journal of Science & Technology Law 69.

Cole, Richard G III, “The Constitutional Insecurity of Secured Smartphones: Unlocking the Current Fourth and Fifth Amendment Safeguards Protecting Secured Smartphones from Law Enforcement Searches” (2018) 39:2 University of La Verne Law Review 173.

Conroy, Amy & Teresa Scassa, “Promoting Transparency While Protecting Privacy in Open Government in Canada” (2015) 53:1 Alberta Law Review 175.

Cook Barr, Allen, “Guardians of Your Galaxy S7: Encryption Backdoors and the First Amendment” (2016) 101:1 Minnesota Law Review 301.

Corken, Erin, “The Changing Expectation of Privacy: Keeping up with the Millennial Generation and Looking toward the Future” (2015) 42:2 North Kentucky Law Review 287.

Corn, Geoffrey S, “Averting the Inherent Dangers of Going Dark: Why Congress Must Require a Locked Front Door to Encrypted Data” (2015) 72:3 Washington and Lee Law Review 1433.

———, “Encryption, Asymmetric Warfare, and the Need for Lawful Access” (2017) 26:2 William Mary Bill Rights Journal 337.

Cosman, Robert W, “A Man’s House Is His Castle-’Beep’: A Civil Law Remedy for the Invasion of Privacy” (1971) 29 Faculty Law Review 3.

Coutros, Gregory, “The Implications of Creating an iPhone Backdoor” (2016) 6:2 National Security Law Brief 81.

Cruess, Jim, “Cost of Admission: One Rubber Stamp - Evaluating the Significance of Investigative Necessity in Wiretap Authorizations after R v Araujo” (2013) 22 Dalhousie Journal of Legal Studies 59.

Currie, Robert J, “Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the ‘Next Frontier’?” (2016) Canadian Yearbook of International Law 63.

———, “Electronic Devices at the Border: The Next Frontier of Canadian Search and Seizure Law?” (2016) 14:2 Canadian Journal of Law & Technology 289.

Czerniawski, James & Connor Boyack, “Reviewing the Privacy Implications of Law Enforcement Access to and Use of Digital Data” (2021) 5:1 Utah Journal of Criminal Law 73.

Dalla Guarda, Nicola, “Digital Encryption and the Freedom from Self-incrimination: Implications for the Future of Canadian Criminal Investigations and Prosecutions” (2014) 61 Crim Law Q 119.

Damaska, Mirjan, “Evidentiary Barriers to Conviction and Two Models of Criminal Procedure: A Comparative Study” (1973) 121 University of Pennsylvania Law Review 506.

Daskal, Jennifer, “Borders and Bits” (2018) 71:1 Vanderbilt Law Review 179.

———, “Law Enforcement Access to Data across Borders: The Evolving Security and Rights Issues” (2016) 8:3 Journal of National Security, Law & Policy 473.

———, “Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0” (2018) 71 Stanford Law Review Online 9.

———, “Privacy and Security Across Borders” (2019) 128 Yale Law Journal Forum 1029.

———, “The Un-Territoriality of Data” (2015) 125:2 Yale Law Journal 326.

———, “Transnational Government Hacking” (2020) 10:3 Journal of National Security Law and Policy 677.

Davoudi, Fariborz, “The Privilege Against Self-Incrimination (Part III)” (2017) 10-04–02 RegQuest.

DeNardis, Laura & Mark Raymond, “The Internet of Things as a Global Policy Frontier” (2017) 51 University of California, Davis 475.

Dennis, Ian H, “Rectitude Rights and Legitimacy: Reassessing and Reforming the Privilege against Self-Incrimination in English Law” (1997) 31:1–3 Israel Law Review 24.

Dheri, Pam & Dave Cobey, “Lawful Access & Encryption in Canada: A Policy Framework Proposal” (2020) 68 Criminal Law Quarterly 430.

Diab, Robert, "The Road Not Taken: Missing Powers to Compel Decryption in Bill C-59, Ticking Bombs, and the Future of the Encryption Debate" (2019) 57:1 Alberta Law Review 267.

Diab, Robert & Marshall Putnam, "Is Password Compulsion Constitutional in Canada? Two Views" (2019) 77:4 Advocate Vancouver Bar Association 513.

Dixit, Pratik Prakash, "Conceptualizing Interaction between Cryptography and Law" (2018) 11:3 NUJS Law Review 327.

Dolhai, George, "Why a New Approach to Privacy Rights and Section 8 of the Charter is Required in the Cyber Age and What It Could Look Like" (2020) 68 Criminal Law Quarterly 29.

Donohue, Laura K, "Customs, Immigration, and Rights: Constitutional Limits on Electronic Border Searches" (2018) 128 Yale Law Journal Forum 961.

Douglass, John, "The Legality of Watering-Hole-Based NITs under International Law" (2017) 2:1 Georgetown Law Technology Review 67.

Dripps, Donald A, "The Substance-Procedure Relationship in Criminal Law" in RA Duff & Stuart Green, eds, *Philos Found Crim Law* (New York: Oxford University Press, 2013).

Dufraimont, Lisa, "Section 13 Immunity After *R v Nedelcu*" (2012) 96 CR (6^{th}) 431.

———, "The Common Law Confessions Rule in the Charter Era: Current Law and Future Directions" (2008) 40 Supreme Court Law Rev (2d) 249.

———, "The Patchwork Principle against Self-Incrimination under the Charter" (2012) 57 Supreme Court Law Review (2d) 241.

Duong, John, "The Intersection of the Fourth and Fifth Amendments in the Context of Encryption Personal Data at the Border" (2009) 2:1 Drexel Law Review 313.

Earls Davis, Peter Alexander, "Decrypting Australia's 'Anti-Encryption' legislation: The meaning and effect of the 'systemic weakness' limitation" (2022) 44 Computer Law & Security Review 1.

Edgett, Sean J, "Double-Clicking on Fourth Amendment Protection: Encryption Creates a Reasonable Expectation of Privacy" (2003) 30:2 Pepperdine Law Review 339.

Ellyson, Laura, "La saisie de données situées dans le nuage en droit criminel canadien" (2019) 17:1 Canadian Journal of Law and Technology 1.

Els, Andrea Scripa, "Artificial Intelligence as a Digital Privacy Protector" (2017) 31:1 Harvard Journal of Law and Technology 217.

Elvy, Stacy-Ann, "Commodifying Consumer Data in the Era of the Internet of Things" (2018) 59 Boston College Law Review 423.

Engel, Joshua A, "Rethinking the Application of the Fifth Amendment to Passwords and Encryption in the Age of Cloud Computing" (2012) 33:3 Whittier Law Review 543.

Etzioni, Amitai, "A Cyber Age Privacy Doctrine: More Coherent, Less Subjective, and Operational" (2015) 80:4 Brooklyn Law Review 1263.

———, "End to End Encryption, the Wrong End" (2016) 67 South California Law Review 561.

Eubank, Rebecca, "Hazy Jurisdiction: Challenges of Applying the Stored Communications Act to Information Stored in the Cloud" (2016) 7:2 George Mason Journal of International Commercial Law 161.

Fakhoury, Hanni, "The Fifth Amendment and Privilege against Compelled Decryption" (2012) 9 Digital Evidence and Electronic Signature Law Review 81.

Farrar, R Thomas, "Aspects of Police Search and Seizure Without Warrant in England and the United States" (1974) 29 University of Miami Law Review 491.

Fehr, Colton, "Criminal Law and Digital Technologies: An Institutional Approach to Rule Creation in a Rapidly Advancing and Complex Setting" (2019) 65:1 McGill Law Journal 67.

———, "Digital Evidence and the Adversarial System: A Recipe for Disaster?" (2018) 16 Canadian Journal of Law and Technology 437.

Fehr, Colton & Jared Biden, "Divorced from (Technological Reality): A Response to the Supreme Court of Canada's Reasons in *R. v. Fearon*" (2015) 20 Canadian Criminal Law Review 93.

Feldman, David, "Considerations on the Emerging Implementation of Biometric Technology" (2003) 25:3 Hastings Communications and Entertainment Law Journal 653.

Findley, Keith, "Toward a New Paradigm of Criminal Justice: How the Innocence Movement Mergers Crime Control and Due Process" (2008) 41 Texas Technology Law Review 133.

Flynn, Abbey, "Physical Fruits vs. Digital Fruits: Why Patane Should Not Apply to the Contents of Digital Devices" (2021) 2021:1 University of Illinois Journal of Law Technology and Policy 1.

Folkinshteyn, Benjamin, "A Witness against Himself: A Case for Stronger Legal Protection of Encryption" (2013) 30 Santa Clara High Technology Law Journal 414.

Force Hill, Jonah, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders" (2014) The Hague Institute for Global Justice, Conference on the Future of Cyber Governance.

Foremski, Tom, "The Battle over Encryption Technologies" (1994) 8 International Yearbook of Law and Computer Technology 311–314.

Forester, Nathan, "Electronic Surveillance, Criminal Investigations, and the Erosion of Constitutional Rights in Canada: Regressive U-Turn of a Mere Bump in the Road towards Charter Justice?" (2010) 73:1 Saskatchewan Law Review 23.

Fraser, David T, "Case Comment: *British Columbia (Attorney General) v. Brecknell*" (2020) 18:1 Canadian Journal of Law and Technology 135.

Fric, Agathon, "Reasonableness as Proportionality: Towards a Better Constructive Interpretation of the Law on Searching Computers in Canada" (2016) 21 Appeal 59.

Friedland, Steven I, "Drinking from the Fire Hose: How Massive Self-Surveillance from the Internet of Things is Changing the Face of Privacy" (2017) 119 West Virginia Law Review 891.

Froomkin, Michael A, "The Constitution and Encryption Regulation: Do We Need a 'New Privacy'?" (1999) 3:1 New York University Journal of Legislation and Public Policy 25.

———, "The Metaphor is the Key: Cryptography, The Clipper Chip, and the Constitution" (1995) 143 University of Pennsylvania Law Review 709.

Froomkin, Michael & Zak Colangelo, "Privacy as Safety" (2020) 95:1 Washington Law Review 141.

Galoob, Stephen R, "Retributivism and Criminal Procedure" (2017) 20:3 New Criminal Law Review 465.

Garcha, Rupinder K, "Nits a No-Go: Disclosing Exploits and Technological Vulnerabilities in Criminal Cases" (2018) 93:4 New York University Law Review 822.

Garrie, Daniel B, Matthew J Armstrong & Donald P Harris, "Voice over Internet Protocol and the Wiretap Act: Is Your Conversation Protected?" (2005) 29:1 Seattle University Law Review 95.

Gerstein, Robert S, "The Self-Incrimination Debate in Great Britain" (1979) 27:1 American Journal of Comparative Law 81.

Geshowitz, Adam M, "Password Protected - Can a Password Save Your Cell Phone from a Search Incident to Arrest" (2011) 96 Iowa Law Review 1125.

Ghappour, Ahmed, "Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web" (2017) 69:4 Stanford Law Review 2075.

Gill, Lex, "Law, Metaphor, and the Encrypted Machine" (2018) 55 Osgoode Hall Law Journal 440.

———, “Law, Metaphor, and the Encrypted Machine” (2018) 55 Osgoode Hall Law Journal 440.

Gimelstein, Shelli, “A Location-Based Test for Jurisdiction over Data: The Consequences for Global Online Privacy” (2018) 2018:1 University of Illinois Journal of Law, Technology and Policy 1.

Gliksberg, Candice, “Decrypting the Fourth Amendment: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Encryption Technology” (2017) 50:4 Loyola Los Angeles Law Review 765.

Gold, Alan D, “If the shoe fits... and wonderfully so: Part VI of the Criminal Code Should be Applied to Digital Communications” (2016) Alan Gold Collect Crim Law Articles.

Goldman, Kara, “Biometric Passwords and the Privilege against Self-Incrimination” (2015) 33 Cardozo Arts & Entertainment Law Journal 211.

Goldstein, Abraham S, “Reflections on Two Models: Inquisitorial Themes in American Criminal Procedure” (1974) 26 Stanford Law Review 1009.

Gonzalez, Olivia, “Cracks in the Armor: Legal Approaches to Encryption” (2019) 2019:1 University of Illinois Journal of Law, Technology and Policy 1.

Gray, David, “A Right to Go Dark” (2019) 72:4 SMU Law Review 621.

Griffiths, John, “Ideology in Criminal Procedure or a Third Model of the Criminal Process” (1970) 79 Yale Law Journal 359.

Hasan, Nader R, “A Step Forward of Just a Sidestep? Year Five of the Supreme Court of Canada in the Digital Age” (2015) 71 Supreme Court Law Review (2d) 439–474.

Hathaway, Oona A et al, “The Law of Cyber-Attack” (2012) 100:4 California Law Review.

Hayes, Liam M, “Smartphone Searches: A Legal Crossroads Between Charter Rights and Law Enforcement” (2018) 66 Criminal Law Quarterly 196.

Hazlett, Katharine B, “The Nineteenth Century Origins of the Fifth Amendment Privilege Against Self-Incrimination” (1998) 42 American Journal of Legal History 235.

Healy, Patrick, “Investigative Detention in Canada” (2005) Criminal Law Review 98.

Herrera, Adam, “Biometric Passwords and the Fifth Amendment: How Technology Has Outgrown the Right to Be Free from Self-Incrimination” (2019) 66:3 UCLA Law Review 778.

Hill-Smith, Micah, “Smartphone Encryption: A Legal Framework for Law Enforcement to Survive the ‘Going Dark’ Phenomenon” (2019) 25 Auckland University Law Review 173.

Hochstrasser, Daniel, "Encryption and the Privilege Against Self-Incrimination: What Happens When a Suspect Refuses to Divulge a Password" (2021) Forthcoming University of New South Wales Law Journal.

Hon, W Kuan & Christopher Millard, "Data Export in Cloud Computing - How Can Personal Data Be Transferred Outside the EEA: The Cloud of Unknowing, Part 4" (2012) 9:1 SCRIPTed Journal of Law, Technology and Society 25.

Hunt, Chris DL, "Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for the Development of Canada's Fledging Privacy Tort" (2011) 37:1 Queens Law Journal 167.

Hurwitz, Justin, "EncryptionCongressMod (Apple + CALEA)" (2017) 30:2 Harvard Journal of Law and Technology 355.

Hutchinson, Melanie, "Unintended Consequences and Australia's Assistance and Access Act 2018 - Is Australia Creating a Technology Based Human Rights Problem?" (2019) 12:47 International In-House Counsel Journal 1.

Iqbal, Mohammad, "Defining Cyberterrorism" (2004) 22:2 John Marshall Journal of Computers and Information Law 397–408.

Jackson, John D, "Silence and Proof: Extending the Boundaries of Criminal Proceedings in the United Kingdom" (2001) 5:3 International Journal of Evidence and Proof 145.

———, "Theories of Truth Finding in Criminal Procedure: An Evolutionary Approach" (1988) 10 Cardozo Law Review 475.

Jackson, Margaret, "Data Protection Regulation in Australia after 1988" (1997) 5:2 International Journal of Law and Information Technology 158.

Jaffer, Jamil N & Daniel J Rosenthal, "Decrypting our Security: A Bipartisan Argument for a Rational Solution to the Encryption Challenge" (2016) 24:2 Catholic University Journal of Law and Technology 273.

James, Carolyn, "Balancing Interests at the Border: Protecting Our Nation and Our Privacy in Border Searches of Electronic Devices" (2010) 27:1 Santa Clara Computer & High Technology Law Journal 219.

Jarone, Joseph, "An Act of Decryption Doctrine: Clarifying the Act of Production Doctrine's Application to Compelled Decryption" (2015) 10 FIU Law Review 767.

Johnson, David R & David Post, "Law and Borders: The Rise of Law in Cyberspace" (1996) 48:5 Stanford Law Review 1367.

Jones, Meg Leta, "Privacy without Screens & the Internet of Other People's Things" (2015) 51 Idaho Law Review 639.

Keenan, Bernard, “State access to encrypted data in the United Kingdom: The ‘transparent’ approach” (2020) 49:3–4 Common Law World Review 223.

Kelsen, Hans, “Droit et état du point de vue d’une théorie pure” (1936) 2 Annales de l’Institut de Droit Comparé de l’Université de Paris 17.

Kerr, Orin S, “An Equilibrium-Adjustment Theory of the Fourth Amendment” (2011) 125:2 Harvard Law Review 476.

———, “Compelled Decryption and the Privilege Against Self-Incrimination” (2019) 97 Texax Law Review 767.

———, “The Fourth Amendment in Cyberspace: Can Encryption Create a Reasonable Expectation of Privacy?” (2001) 33:2 Connecticut Law Review 503.

Kerr, Orin S & Sean D Murphy, “Government Hacking to Light the Dark Web: What Risks to International Relations and International Law?” (2017) 70 Stanford Law Review Online 58.

Kerr, Orin S & Bruce Schneier, “Encryption Workarounds” (2018) 106 Georgetown Law Journal 989.

Kiok, Jeffrey, “Missing the Metaphor: Compulsory Decryption and the Fifth Amendment” (2015) 24 Boston University Public Interest Law Journal 53.

Koutros, Nicholas & Julien Demers, “Big Brother’s Shadow: Decline in Reported Use of Electronic Surveillance by Canadian Federal Law Enforcement” (2013) 11 Canadian Journal of Law and Technology.

Kraft, Timothy J, “Big Data Analytics, Rising Crime, and Fourth Amendment Protections” (2017) 2017:1 University of Illinois Journal of Law, Technology and Policy 249.

Larkin, John ED, “Compelled Production of Encrypted Data” (2012) 14 Vanderbilt Journalf of Entertainment and Technology Law 253.

Leamon, Madeline, “Unlocking the Right against Self-Incrimination: A Predictive Analysis of 21st Century Fifth Amendment Jurisprudence” (2019) 64:2 Wayne Law Review 583.

Lear, Shannon, “The Fight over Encryption: Reasons Why Congress Must Block the Government from Compelling Technology Companies to Create Backdoors into Their Devices” (2018) 66:2 Cleveland State Law Review 443.

Lebowitz, Jason, “Technology and Individual Privacy Rights: The Fourth Amendment Implication of Exploiting Zero-Day Vulnerabilities for Domestic Investigations” (2015) 47:1 Columbia Human Rights Law Review 242.

Lemus, Efren, "When Fingerprints Are Key: Reinstating Privacy to the Privilege against Self-Incrimination in Light of Fingerprint Encryption in Smartphones" (2017) 70 SMU Law Review 533.

Lichlyter, Lydia, "Encryption, Guns, and Paper Shredders: Analogical Reasoning with Physically Dangerous Technologies" (2017) 31:1 Harvard Journal of Law and Technology 259.

Liguori, Carlos, "Exploring Lawful Hacking as a Possible Answer to the 'Going Dark' Debate" (2020) 26:2 Michigan Technology Law Review 317.

Lotrionte, Nicolette, "The Sky's the Limit - The Border Search Doctrine and Cloud Computing" (2013) 78:2 Brooklyn Law Review 663.

Lowell, Karen G, "Civil Liberty or National Security: The Battle over iPhone Encryption" (2017) 33:2 Georgia State University Law Review 485.

Luna, Erik, "A Place for Comparative Criminal Procedure" (2003) 42 Brandeis Law Journal 277.

Ly, Branden, "Never Home Alone: Data Privacy Regulations for the Internet of Things" (2017) 2017 University of Illinois Journal of Law, Technology and Policy 539.

Lyon, Nathan D, "Compelling Decryption of a Smartphone under the Fifth Amendment" (2021) 5:1 Utah Journal of Criminal Law 57.

MacNish, Kevin, "Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World" (2018) 35:2 Journal of Appl Philosophy 417.

Mahoney, Michael S, "Compelling the Production of Passwords: Government's Ability to Compel the Production of Passwords Necessary to the Discovery of Encrypted Evidence in Criminal Proceedings, Merely a Choice of Words" (2003) 6 TM Cool Journal of Practical & Clinical Law 83.

Makker, Sona R, "Overcoming Foggy Notions of Privacy: How Data Minimization Will Enable Privacy in the Internet of Things" (2017) 85:4 UMKC Law Review 895.

Mann, Monique, Angela Daly & Adam Molnar, "Regulatory arbitrage and transnational surveillance: Australia's extraterritorial assistance to access encrypted communications" (2020) 9:3 Internet Policy Review 1.

Manpearl, Eric, "Preventing Going Dark: A Sober Analysis and Reasonable Solution to Preserve Security in the Encryption Debate" (2017) 28:1 University of Florida Journal of Law and Public Policy 65.

———, "The International Front of the Going Dark Debate" (2018) 22:4 Virginia Journal of Law & Technology 158.

Marcus, Paul & Vicky Waye, "Australia and the United States: Two Common Criminal Justice Systems Uncommonly at Odds" (2003) 12:1 Tulane Journal of International and Comparative Law 27.

Mayer, Jonathan, "Government Hacking" (2017) 127:3 Yale Law Journal 570.

MacDonald, Stuart, "Constructing a Framework for Criminal Justice Research: Learning from Packer's Mistakes" (2008) 11:2 New Criminal Law Review 257.

McCarthy, Ian J, "iOS Fear the Government: Closing the Back Door on Governmental Access" (2017) 49:1 University of Toledo Law Review 179.

McGarrity, Nicola & Keiran Hardy, "Digital surveillance and access to encrypted communications in Australia" (2020) 49:3–4 Common Law World Review 160.

McGregor, Nathan K, "Weak Protections of Strong Encryption: Passwords, Privacy, and the Fifth Amendment Privilege" (2010) 12 Vanderbilt Journal of Entertainment and Technology Law 581.

McInerney, Pat, "The Privilege against Self-Incrimination from Early Origins to Judges' Rules: Challenging the Orthodox View" (2014) 18 International Journal of Evidence and Proof 101.

McLaughlin, Paul, "Crypto Wars 2.0: Why Listening to Apple on Encryption Will Make America More Secure" (2016) 30:2 Temple International Comparative Law Journal 353.

Mendoza, Eduardo R, "Network Investigation Techniques: Government Hacking and the Need for Adjustment in the Third-Party Doctrine" (2017) 49:1 St Marys' Law Journal 237.

Metz, Harrison, "Your Device is Disabled: How and Why Compulsion of Biometrics to Unlock Devices Should Be Protected Under the Fifth Amendment Privilege" (2019) 53:2 Valparaiso University Law Review 427.

Miller, Thomas Mann, "Digital Border Searches after Riley v California" (2015) 90:4 Washington Law Review 1943.

Mischenko, Lidiya, "The Internet of Things: Where Privacy and Copyright Collide" (2016) 33 Santa Clara Computer & High Technology Law Journal 90.

Mizrahi, Sarit K, "Ontario's New Invasion of Privacy Torts: Do They Offer Monetary Redress for Violations Suffered via the Internet of Things?" (2018) 8:1 Western Journal of Legal Studies 3.

———, "The Dangers of Sharing Cloud Storage: The Privacy Violations Suffered by Innocent Cloud Users during the Course of Criminal Investigations in Canada and the United States" (2017) 25 Tulane Journal of International and Comparative Law 303.

Mohan, Vivek & John Willasenor, "Decrypting the Fifth Amendment: The Limits of Self-Incrimination in the Digital Era" (2012) 15 University of Pennsylvania Journal of Constitutional Law Heightened Scrutiny 11.

Moore, Michael S, Placing Blame: A General Theory of the Criminal Law (Oxford: Oxford University Press, 2010).

Murphy, Cian C, "The Crypto-Wars Myth: The reality of state access to encrypted communications" (2020) 49:3–4 Common Law World Review 245.

Myers Morrison, Caren, "Passwords, Profiles, and the Privilege Against Self-Incrimination: Facebook and the Fifth Amendment" (2012) 65 Arkansas Law Review 133.

Nagareda, Richard A, "Compulsion 'To Be a Witness' and the Resurrection of Boyd" (1999) 74 NYU Law Review 1575.

Ng, Rudy, "Catching up to Our Biometric Future: Fourth Amendment Privacy Rights and Biometric Identification Technology" (2005) 28:3 Hastings Communications and Entertainment Law Journal 425.

Nguyen, Titi, "Computer Security and the Law: Regulating the Export of Encryption" (2001) 1 Law Society Review UCSB 49.

Oddo, Adrianna, "Being Forced to Code in the Technology Era as a Violation of the First Amendment Protection against Compelled Speech" (2018) 67:1 Catholic University Law Review 211.

Ohm, Paul, "The Investigative Dynamics of the Use of Malware by Law Enforcement" (2017) 26:2 William and Mary Bill of Rights Journal 303.

Opderbeck, David W, "Encryption Policy and Law Enforcement in the Cloud" (2017) 49:5 Connecticut Law Review 1657.

———, "The Skeleton in the Hard Drive: Encryption and the Fifth Amendment" (2018) 70 Florida Law Review 883.

Osborn, Debra, "Suppressing the Truth: Judicial Exclusion of Illegally Obtained Evidence in the United States, Canada, England and Australia" (2000) 7:4 Murdoch University Electronic Journal Law.

Osula, Anna-Maria, "Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study" (2016) 24:4 International Journal of Law and Information Technology 343.

Paciocco, David M, "Self-Incrimination and the Case to Meet: The Legacy of Chief Justice Lamer" (2000) 5 Canadian Criminal Law Review 63.

Packer, Herbert L, "Two Models of the Criminal Process" (1964) 113 University of Pennsylvania Law Review 1.

Palfreyman, Brendan M, “Lessons from the British and American Approaches to Compelled Decryption” (2009) 75 Brooklyn Law Review 345.

Parsons, Christopher & Adam Molnar, “Government Surveillance Accountability: The Failures of Contemporary Canadian Interception Reports” (2018) 16 Canadian Journal of Law and Technology 143.

Pelletier, Benoît, “La protection de la vie privée au Canada” (2001) 35 RJT 485–522.

Penney, Steven, “Consent Searches for Electronic Text Communications: Escaping the Zero-Sum Trap” (2018) 56 Alberta Law Review 1.

———, “Updating Canada’s Communications Surveillance Laws: Privacy and Security in the Digital Age” (2008) 12 Canadian Criminal Law Review 115.

———, “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” (2003) 48 Criminal Law Quarterly 249.

Penney, Steven & Dylan Gibbs, “Law Enforcement Access to Encrypted Data: Legislative Responses and the Charter” (2017) 63 McGill Law Journal 201.

Phelps, Jenna, “It is Only a Fingerprint: Biometric Compulsion and the Fifth Amendment” (2020) 89:2 UMKC Law Review 461.

Pinto, Minerva, “The Future of the Foregone Conclusion Doctrine and Compelled Decryption in the Age of Cloud Computing” (2016) 25:1 Temple Political & Civil Rights Law Review 223.

Pool, Ronald LD & Bart HM Custers, “The Police Hack Back: Legitimacy, Necessity and Privacy Implications of the Next Step in Fighting Cybercrime” (2017) 25:2 European Journal of Crime, Criminal Law and Criminal Justice 123.

Postema, Gerald J, “The Principle of Utility and the Law of Procedure: Bentham’s Theory of Adjudication” (1977) 11 Georgia Law Review 1393 at 1395.

Potapchuk, John L, “A Second Bite at the Apple: Federal Courts’ Authority to Compel Technical Assistance to Government Agents in Accessing Encrypted Smartphone Data under the All Writs Act” (2016) 57:4 Boston College Law Review 1403.

Poudel, Swaroop, “Internet of Things: Underlying Technologies, Interoperability, and Threats to Privacy and Security” (2016) 31 Berkeley Technology Law Journal 997.

Raj, Matthew & Russ Marshall, “Examining the Legitimacy of Police Powers to Search Portable Devices in Queensland” (2019) 38:1 University of Queensland Law Journal 99.

Rangaviz, David Rassoul, “Compelled Decryption & State Constitutional Protection Against Self-Incrimination” (2020) 57:1 American Criminal Law Review 157.

Ratushny, Ed, “Is There a Right against Self-Incrimination in Canada?” (1973) 19:1 McGill Law Journal 1.

Redfern, Ariel N, “Face It - The Convenience of a Biometric Password May Mean Forfeiting Your Fifht Amendment Rights” (2021) 125:2 Pennsylvania State Law Review 597.

Reitinger, Nathan, “Faces and Fingers: Authentication” (2020) 20 Journal of High Technology Law 61.

Reitinger, Phillip R, “Compelled Production of Plaintext and Keys” (1996) University of Chicago Legal Forum 171.

Rengel, Alexandra, “Privacy as an International Human Right and the Right to Obscurity in Cyberspace” (2014) 2:2 Groningen Journal of International Law 33–54.

Roach, Kent, “Four Models of the Criminal Process” (1999) 89:2 Journal of Criminal Law & Criminology 671.

Rowland, Rebecca M, “Border Searches of Electronic Devices” (2019) 97:2 Washington University Law Review 545.

Rozenshtein, Alan Z, “Wicked Crypto” (2019) 9:5 UC Irvine Law Review 1181.

Ryan, Jill M, “Freedom to Speak Unintelligibly: The First Amendment Implications of Government-Controlled Encryption” (1996) 4:3 William & Mary Bill of Rights Journal 1165.

Sacharoff, Laurent, “Unlocking the Fifth Amendment: Passwords and Encrypted Devices” (2018) 87 Fordham Law Review 203.

———, “What Am I Really Saying When I Open My Smartphone: A Response to Orin S. Kerr” (2018) 97 Texas Law Review Online 63.

Sales, Erin M, “The Biometric Revolution: An Erosion of the Fifth Amendment Privilege to Be Free from Self-Incrimination” (2014) 69 University of Miami Law Review 193.

Schiff Berman, Paul, “Legal Jurisdiction and the Deterritorialization of Data” (2018) 71 Vanderbilt Law Review 11.

Shah, Reema, “Law Enforcement and Data Privacy – A Forward-Looking Approach” (2015) 125 Yale Law Journal 543.

Sherman, Kelsey, “Biometrics: The Future Is in Your Hands” (2017) 50:4 Loyola Los Angeles Law Review 663.

Shweiki, Opher & Youli Lee, “Compelled Use of Biometric Keys to Unlock a Digital Device: Deciphering Recent Legal Developments” (2019) 67 US Attorney’s Bulletin 23.

Skolnik, Terry, “The Suspicious Distinction between Reasonable Suspicion and Reasonable Grounds to Believe” (2016) 47:1 Ottawa Law Review 227.

Skorvanek, Ivan et al, “‘My Computer Is My Castle’: New Privacy Frameworks to Regulate Police Hacking” (2019) 2019:4 Brigham Young University Law Review 997.

Soares, Nicholas, “The Right to Remain Encrypted: The Self-Incrimination Doctrine in the Digital Age” (2012) 49 American Criminal Law Review 2001.

Solakian, Lea M, “The Key to Compelled Decryption: Beyond a Reasonable Doubt” (2021) 27:2 Widener Law Review 219.

Solove, Daniel J, “A Taxonomy of Privacy” (2006) 154:3 University of Pennsylvania Law Review 477.

———, “Conceptualizing Privacy” (2002) 90 California Law Review 1087.

———, “I’ve Got Nothing to Hide and Other Misunderstandings of Privacy” (2007) 44:4 San Diego Law Review 745.

Stewart, Hamish, “Normative Foundations for Reasonable Expectations of Privacy” (2011) 54 Supreme Court Law Review (2d) 335.

———, “The Confessions Rule and the Charter” (2009) 54:3 McGill Law Journal 517.

Stransky, Steven G, “Border Searches and the Limits of Encryption in Protecting Privileged Information” (2018) 44:4 Litigation 15.

Stribopoulos, James, “In *Search* of Dialogue: The Supreme Court, Police Powers and the *Charter*” (2005) 32 Queen’s Law Journal 1.

———, “Sniffing Out the Ancillary Powers Implications of the Dog Sniff Cases” (2009) 47 Supreme Court Law Review: Osgoode’s Annual Constitutional Cases Conference 35.

Stuart, Don, “Vagueness, Inconsistency and Less Respect for Charter Rights of Accused at the Supreme Court in 2012-2013” (2013) 63 Supreme Court Law Review: Osgoode’s Annual Constitutional Cases Conference 441.

Stuesser, Lee, “*R v S.A.B.*: Putting “Self-Incrimination” in Context” (2004) 42:2 Alta L Rev 543.

Swire, Peter & Kenesa Ahmad, “Encryption and Globalization” (2012) 13:2 Columbia Science & Technology Law Review 416.

Taylor, Steven B, “Can You Keep a Secret: Some Wish to Ban Encryption Technology for Fears of Data Going Dark” (2016) 19 SMU Science & Technology Law Review 215–250.

Terzian, Dan, “Forced Decryption as Equilibrium - Why It’s Constitutional and How Riley Matters” (2015) 109:4 Northwest University Law Review 1131.

———, “The Fifth Amendment, Encryption, and the Forgotten State Interest” (2014) 61 UCLA Law Review Discourse 298–313.

Thai, Joseph T, “Is Data Mining Ever a Search Under Justice Stevens’s Fourth Amendment?” (2006) 74:4 Fordham Law Review 1731.

Theophilopoulos, Constantine, “The Influence of American and English Law on the Interpretation of the South African Right to Silence and the Privilege against Self-Incrimination” (2005) 19:2 Temple International & Comparative Law Journal 387.

Thierer, Adam D, “The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation” (2014) 21 Richmond Journal of Law & Technology 1.

Thornburn, Malcolm, “Criminal Law as Public Law” in RA Duff & Stuart Green, eds, *Philos Found Crim Law* (Oxford; New York: Oxford University Press, 2011) 543.

Tien, Lee, “Doors, Envelopes, and Encryption: The Uncertain Role of Precautions in Fourth Amendment” (2005) 54:3 DePaul Law Review 873.

Tran, Alexander H, “The Internet of Things and Potential Remedies in Privacy Tort Law” (2017) 50 Columbia Journal of Law & Social Problems 263.

Turner, Anne, “Wiretapping Smart Phones with Rotary-Dial Phones’ Law: How Canada’s Wiretap Law Is in Desperate Need of Updating” (2017) 40 Manitoba Law Journal 249.

Twining, William, “Evidence and Legal Theory” (1984) 47:3 Modern Law Review 261.

Ungberg, Andrew J, “Protecting Privacy through a Responsible Decryption Policy” (2009) 22 Harvard Journal of Law & Technology 537.

Uresk, Carissa A, “Compelling Suspects to Unlock Their Phones: Recommendations for Prosecutors and Law Enforcement” (2021) 46:2 Brigham Young University Law Review 601.

Vandenberg, Dustin Taylor, “Encryption Served Three Ways: Disruptiveness as the Key to Exceptional Access” (2017) 32 Berkeley Technology Law Journal 531.

van den Hoven van Genderen, Robert, “Privacy and Data Protection in the Age of Pervasive Technologies in AI and Robotics” (2017) 3:3 European Data Protection Law Review (EDPL) 338.

Vassilaki, IE, “Crime Investigation versus Privacy Protection - An Analysis of Colliding Interests” (1994) 2:1 European Journal of Crime, Criminal Law and Criminal Justice 39.

Vayas, Antonio, “Say Cheese: How the Fourth Amendment Fails to Protect Your Face” (2021) 51:5 Seton Hall Law Review 1639.

Verdon, Ashley H, “International Travel with a Digital Briefcase: If Customs Officials Can Search a Laptop, Will the Right against Self-Incrimination Contravene This Authority” (2009) 37 Pepperdine Law Review 105.

Victory, Hillary, “Big Brother is at Your Back Door: An Examination of the Effect of Encryption Regulation on Privacy and Crime” (2000) 18 Journal of Computer & Information Law 825.

Volini, Anthony G & Farzana Ahmed, “Strategies to Deter Child Pornography in the Absence of a Mandatory Encryption Back Door: Tipster Programs, a Licensed Researched System, Compelled Password Production, & Private Surveillance” (2022) 32:1 DePaul Journal of Art, Technology and Intellectual Property Law 1.

Wachtel, Michael, “Give Me Your Password Because Congress Can Say So: An Analysis of Fifth Amendment Protection Afforded Individuals regarding Compelled Production of Encrypted Data and Possible Solutions to the Problem of Getting Data from Someone’s Mind” (2013) 14 Pittsburg Journal of Technology Law and Policy 44.

Wainscott, Alexa, “A Golden Key to Pandora’s Box: The Security Risks of Government-Mandated Backdoors to Encrypted Communications” (2017) 44:1 North Kentucky Law Review 57.

Walker, Kiel, “La protection contre l’auto-incrimination testimoniale au Canada et le droit québécois: Quoi protège qui?” (2015) 46:2 Ottawa Law Review 315.

Warren, Samuel & Louis Dembitz Brandeis, “The Right to Privacy” (1890) 4 Harvard Law Review 193.

Weber, Dane Bryce, “The Cybernetic Sea: Australia’s Approach to the Wave of Cybercrime” (2014) 14 QUT Law Review 52.

Weber, Matthew J, “Warning - Weak Password: The Courts’ Indecipherable Approach to Encryption and the Fifth Amendment” (2016) 2016:2 University of Illinois Journal of Law, Technology and Policy 455.

Weigel, Nicholas A, “Apple’s ‘Communication Safety’ Feature for Child Users: Implications for Law Enforcement’s Ability to Compel iMessage Decryption” (2022) 25:2 Stanford Technology Law Review 210.

West, Leah & Craig Forcese, “Twisted Into Knots: Canada’s Challenges in Lawful Access to Encrypted Communications” (2019) Ottawa Faculty Law Working Paper No 2019-38.

Whitling, NJ, “Wiretapping, Investigative Necessity, and the Charter” (2002) 46:1 Criminal Law Quarterly 89.

Wiseman, Timothy A, "Encryption, Forced Decryption, and the Constitution" (2015) 11 I/S: Journal of Law and Policy for the Information Society 525–575.

Wolfe, D Forest, "The Government's Right to Read: Maintaining State Access to Digital Data in the Age of Impenetrable Encryption" (2000) 49 Emory Law Journal 711–744.

Zaia, Reem, "Constitutional and Quasi-Constitutional Privacy Protections: In Defence of a Heightened Expectation of Privacy for Young People Participating in the Digital World" (2020) 68 Criminal Law Quarterly 362.

Zallone, Raffaele, "Here, There and Everywhere: Mobility Data in the EU (Help Needed: Where is Privacy?)" (2013) 30:1 Santa Clara High Technology Law Journal 57.

Zarefsky, Jacob, "The Precarious Balance between National Security and Individual Privacy: Data Encryption in the Twenty-First Century" (2021) 23 Tulane Journal of Technology and Intellectual Property 179.

Zweig, Arnulf, "Retributivism, Resentment and Amnesty" (1995) 3 Jahrbuch fur Recht und Ethik 267.

Secondary Materials: Reports and Online Sources

Abelson, Harold et al, *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to all Data and Communications*, by Harold Abelson et al (Cambridge: MIT Cybersecurity and Internet Policy Research Initiative, 2015).

Ad-hoc Subgroup on Transborder Access and Jurisdiction, *Transborder access to data and jurisdiction: Options for further action by the T-CY*, by Ad-hoc Subgroup on Transborder Access and Jurisdiction (Council of Europe - Cybercrime Convention Committee (T-CY), 2014).

Amazon, "Protecting data using encryption", online: *Amazon* <https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html>.

Amnesty International, *Encryption: A Matter of Human Rights* (Amnesty International, 2016).

Apple, "About Face ID Advanced Technology, (27 April 2022), online: *Apple Support* <https://support.apple.com/en-us/HT208108>.

———, "Encrypt Mac data with FileVault", online: *Apple Support* <https://support.apple.com/en-ca/guide/mac-help/mh11785/mac>.

———, "How does FileVault encryption work on a Mac?", online: *Apple Support* <https://support.apple.com/en-ca/guide/mac-help/flvlt001/12.0/mac/12.0>.

———, "Use FileVault to encrypt the startup disk on your Mac", (18 November 2018), online: *Apple Support* <https://support.apple.com/en-ca/HT204837>.

Arif, Rauf, "In The Post COVID-19 World, Zoom Is Here To Stay" (2021) Forbes, online: <https://www.forbes.com/sites/raufarif/2021/02/26/in-the-post-covid-19-world-zoom-is-here-to-stay/?sh=3a9c190055b5>.

Australian Law Reform Commission*, Traditional Rights and Freedoms – Encroachments by Commonwealth LS; Final Report* (Sydney: Australian Law Reform Commission (ALRC), 2015).

AxCrypt, "Features", online: *AxCrypt* <https://axcrypt.net/>.

Bayern, Macy, "Why 72% of people still recycle passwords", (18 July 2019), online: *TechRepublic* <https://www.techrepublic.com/article/why-72-of-people-still-recycle-passwords/#:~:text=Users%20recycle%20the%20same%20password,to%20a%20Security.org%20report.>.

BBC News, "Jamal Khashoggi: All you need to know about Saudi journalist's death", (24 February 2021), online: *BBC News* <https://www.bbc.com/news/world-europe-45812399>.

Bhuiyan, Johana, "Facebook gave police their private data. Now, this duo face abortion charges", (10 August 2022), online: *The Guardian* <https://www.theguardian.com/us-news/2022/aug/10/facebook-user-data-abortion-nebraska-police>.

Bocetta, Sam, "Australia's New Anti-Encryption Law is Unprecedented and Undermines Global Privacy", (14 February 2019), online: *Foundation for Economic Education* <https://fee.org/articles/australia-s-unprecedented-encryption-law-is-a-threat-to-global-privacy/>.

Boxberger, Darryl, "How to have your iPhone erase all data after 10 failed passcode attempts in iOS 15", (4 March 2022), online: *Apple Insider* <https://appleinsider.com/articles/22/03/04/how-to-have-your-iphone-erase-all-data-after-10-failed-passcode-attempts-in-ios-15>.

Buchanan, Bill, "So What Does a Modern Encryption Key Look Like?", (11 October 2018), online: *Medium* <https://medium.com/asecuritysite-when-bob-met-alice/so-what-does-a-modern-encryption-key-look-like-1c49efde9197>.

Canadian Association of Chiefs of Police, *Resolutions Adopted at the 111th Annual Conference – Resolution #03-2016 – Reasonable Law to Address the Impact of Encrypted and Pass-Word Protected Electronic Devices* (Ottawa, Canada: Canadian Association of Chiefs of Police).

Cannataci, Joseph, *Mandate of the Special Rapporteur on the right to privacy* (2018), online: *Office of the High Commissioner for Human Rights* <https://www.ohchr.org/sites/default/files/O_LAUS_6.2018.pdf>.

Cherry, Paul, "Montreal Mafia: Project Clemenza screeches to a halt as cases stayed", (17 July 2017), online: *Montreal Gazette* <https://montrealgazette.com/news/local-news/montreal-mafia-project-clemenza-screeches-to-a-halt-as-cases-

stayed#:~:text=A%20lengthy%20investigation%20into%20drug,against%20them%20only%20last%20year.>.

Clark, Mitchell, "NSO's Pegasus spyware: here's what we know", (23 July 2021), online: *The Verge* <https://www.theverge.com/22589942/nso-group-pegasus-project-amnesty-investigation-journalists-activists-targeted>.

Cloudflare, "What is HTTPS?", online: *Cloudflare* <https://www.cloudflare.com/learning/ssl/what-is-https/>.

Comey, James B, *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?* (Brookings Institution, 2014).

Cook, Tim, "A Message to Our Customers", (16 February 2016), online: *Apple* <https://www.apple.com/customer-letter/>.

Corder, Mike, "European police crack encrypted phones, arrest hundreds", *Washington Post* (2 July 2020), online: <https://www.washingtonpost.com/world/europe/french-dutch-police-bust-encrypted-criminal-communications/2020/07/02/ff664844-bc55-11ea-97c1-6cf116ffe26c_story.html>.

Council of Europe, "Chart of signatures and ratifications of Treaty 224", (5 August 2022), online: *Council of Europe* <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224>.

Cox, Joseph, "The FBI Tried to Plant a Backdoor in an Encrypted Phone Network", (18 September 2019), online: *Vice* <https://www.vice.com/en_ca/article/pa73dz/fbi-tried-to-plant-backdoor-in-encrypted-phone-phantom-secure>.

Cybercrime Convention Committee (T-CY), "T-CY Guidance Note # 3 - Transborder access to data (Article 32)", (3 December 2014), online: *Council of Europe* <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726a>.

Czeskis, Alexei et al, "Defeating Encrypted and Deniable File Systems: TrueCrypt v5.1a and the Case of the Tattling OS and Applications" (2008) 3rd Usenix Workshop on Hot Topics in Security, online: <https://www.schneier.com/academic/archives/2008/01/defeating_encrypted.html>.

Dalhousie University, "Acceptable Use Policy", (February 2020), online: *Dalhousie University* <https://cdn.dal.ca/content/dam/dalhousie/pdf/dept/university_secretariat/policy-repository/Acceptable%20Use%20Policy%20Feb%202020.pdf>.

Department of Justice - Office of Public Affairs, "United States and Canada Welcome Negotiations of a CLOUD Act Agreement", (22 March 2022), online: *US Department of Justice* <https://www.justice.gov/opa/pr/united-states-and-canada-welcome-negotiations-cloud-act-agreement>.

Déziel, Pierre-Luc, Karim Benyekhlef & Eve Gaumond, *Repenser la protection des renseignements personnels à la lumière des défis soulevés par l'IA* (Laval, Québec, Canada: Observatoire international sur les impacts sociétaux de l'IA et du numérique, 2020).

Dufresne, Philippe, "Appearance before the Standing Committee on Access to Information, Privacy and Ethics (ETHI) on the Study of Device Investigation Tools Used by the RCMP", (8 August 2022), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2022/parl_sub_220808/>.

Dupont, Benoît et al, *Artificial Intelligence in the Context of Crime and Criminal Justice*, by Benoît Dupont et al (Korean Institute of Criminology, 2018).

Dupuis, Tanya et al, "Legislative Summary of Bill C-59: An Act respecting national security measures", (3 June 2019), online: *Parliament of Canada* <https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/LegislativeSummaries/421C59E>.

Encyclopedia Britannica, *VoIP communications* (2022), online <https://www.britannica.com/technology/VoIP>.

ENISA & EUROPOL, "On lawful criminal investigation that respects 21st Century data protection", (20 May 2016), online: <https://www.europol.europa.eu/cms/sites/default/files/documents/on_lawful_criminal_investigation_respecting_21st_century...%20%281%29.pdf>.

European Commission, "E-evidence – Cross-border access to electronic evidence", (2019), online: *Eur Comm* <https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en>.

Ford, Antwanya & LaTia Hutchinson, "Full disk encryption: do we need it?", (18 January 2018), online: *CSO Online* <https://www.csoonline.com/article/3247707/full-disk-encryption-do-we-need-it.html>.

Garland, Randy, "Encryption vs. Password Protection: A Matter of Acceptable Risk", (12 September 2014), online: *LinkedIn* <https://www.linkedin.com/pulse/20140912130912-9768674-encryption-vs-password-protection-a-matter-of-acceptable-risk/>.

Gartenberg, Chaim, "Facebook reportedly avoids US government wiretap of Messenger voice calls", (28 September 2018), online: *The Verge* <https://www.theverge.com/2018/9/28/17915902/facebook-messenger-protected-us-government-wiretap-requests>.

Gill, Lex, Tamir Israel & Christopher Parsons, *Shining a Light on the Encryption Debate: A Canadian Field Guide*, by Lex Gill, Tamir Israel & Christopher Parsons (Toronto: The Citizen Lab and the Canadian Internet Policy & Public Interest Clinic, 2018).

Global Affairs Canada, “Export Controls on Cryptographic Goods”, (23 December 1998), online: *Global Affairs Canada* <https://www.international.gc.ca/controls-controles/systems-systemes/excol-ceed/notices-avis/113.aspx?lang=eng>.

Google, “Global Locations – Regions & Zones”, online: *Google Cloud* <https://cloud.google.com/about/locations>.

Government of Canada, “Directive on Service and Digital”, (6 May 2022), online: *Government of Canada* <https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32601>.

———, “Guideline on Service and Digital”, (23 November 2021), online: *Government of Canada* <https://www.canada.ca/en/government/system/digital-government/guideline-service-digital.html>.

Government of the United Kingdom, “Police powers to stop and search: your rights”, online: *GovUK* <https://www.gov.uk/police-powers-to-stop-and-search-your-rights>.

Grace Johansen, Alison, “What is a Trojan? Is it a virus or is it malware?”, (24 July 2020), online: *Norton* <https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html>.

Greenberg, Andy, “Hacker Lexicon: What Is Perfect Forward Secrecy?”, (28 November 2016), online: *Wired* <https://www.wired.com/2016/11/what-is-perfect-forward-secrecy/>.

———, “Hacker Lexicon: What Is the Signal Encryption Protocol?”, (29 November 2020), online: *Wired* <https://www.wired.com/story/signal-encryption-protocol-hacker-lexicon/>.

Hasan, Nader R & Stephen Aylward, “Password protection a crucial Charter right”, (23 August 2016), online: *The Star* <https://www.thestar.com/opinion/commentary/2016/08/23/password-protection-a-crucial-charter-right.html>.

Hanson, Sara, "*R v Nedelcu*: The Right Against Self-Incrimination and the Return to the Unworkable Distinction" (24 November 2012), online: *The Court* <http://www.thecourt.ca/r-v-nedelcu-the-right-against-self-incrimination-and-the-return-to-the-unworkable-distinction/>.

Hilts, Andrew, “Ciphertext”, (16 May 2018), online: *Citiz Lab* <https://citizenlab.ca/2018/05/shining-light-on-encryption-debate-canadian-field-guide/ciphertext/>.

Hosenball, Mark, “FBI paid under $1 million to unlock San Bernardino iPhone: sources”, *Reuters* (4 May 2016), online: <https://www.reuters.com/article/us-apple-encryption/fbi-paid-under-1-million-to-unlock-san-bernardino-iphone-sources-idUSKCN0XQ032>.

IBM, “Password guidelines”, (7 April 2022), online: *IBM* <https://www.ibm.com/docs/en/aix/7.2?topic=passwords-password-guidelines>.

IBM Cloud Education, "IaaS versus PaaS versus SaaS", (2 September 2021), online: *IBM* <https://www.ibm.com/cloud/learn/iaas-paas-saas>.

Jahn, Jessica, "Canada's Future CLOUD Act Agreement with the United States", (29 March 2022), online: *International Centre for Criminal Law Reform & Criminal Justice Policy ICCLR* <https://icclr.org/2022/03/29/canadas-future-cloud-act-agreement-with-the-united-states/>.

———, "Canada's Position at the UN Cybercrime Treaty Negotiations", (2 March 2022), online: *International Centre for Criminal Law Reform & Criminal Justice Policy ICCLR* <https://icclr.org/2022/03/02/canadas-position-at-the-un-cybercrime-treaty-negotiations/>.

Justice Canada, *Evaluation of the Investigative Powers for the 21st Century Initiative – Final Report*, by Justice Canada (Ottawa, Canada: Justice Canada, 2020).

Karp, Paul, "Australia's world-first anti-encryption law should be overhauled, independent monitor says", (9 July 2020), online: *The Guardian* <https://www.theguardian.com/australia-news/2020/jul/09/australias-world-first-anti-encryption-law-should-be-overhauled-independent-monitor-says>.

Kaspersky, "Kaspersky Lab Finds Over Half of Consumers Don't Password-Protect their Mobile Devices", (2018), online: *Kaspersky* <https://usa.kaspersky.com/about/press-releases/2018_kaspersky-lab-finds-over-half-of-consumers-don-t-password-protect-their-mobile-devices>.

———, "Kaspersky Lab's File Level Encryption Technology", (2013), online: *Kaspersky* <https://media.kaspersky.com/en/business-security/Kaspersky-File-Level-Encryption-Technology.pdf>.

Katwala, Amit, "Quantum computing and quantum supremacy, explained", (5 March 2020), online: *Wired* <https://www.wired.co.uk/article/quantum-computing-explained>.

———, "We're calling it: PGP is dead", (17 May 2018), online: *Wired* <https://www.wired.co.uk/article/efail-pgp-vulnerability-outlook-thunderbird-smime>.

———, "Quantum computers will change the world (if they work)" *Wired* (5 March 2020), online: <https://www.wired.co.uk/article/quantum-computing-explained>.

Kaye, David, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, by David Kaye, UN Doc A/HRC/29/32 (UNHRC, 29th Sess., 2015).

Kerr, Orin, "The surprising implications of the Microsoft/Ireland warrant case", *Washington Post* (29 November 2016), online: <https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/11/29/the-surprising-implications-of-the-microsoftireland-warrant-case/>.

Koomen, Maria, *The Encryption Debate in the European Union: 2021 Update* (Washington, DC: Carnegie Endowment for International Peace, 2021).

Koops, Bert-Jaap & Morag Goodwin, "Cyberspace, the Cloud and Cross-Border Criminal Investigation: The Limits and Possibilities of International Law" (2014) Tilburg Institute for Law, Technology, and Society CTLD – Center for Transboundary Legal Development, online: <https://deliverypdf.ssrn.com/delivery.php?ID=559124089121125007073083097099093124063062077093054032068075011087090105106120006093033098026038045017119075006074066081067122025059009008018097069091096069070086106023000046125105097008098102025119067017091065004030023123112094082070123098074089092026&EXT=pdf&INDEX=TRUE>.

Krishnamurthy, Vivek, "Cloudy with a Conflict of Laws" (2016) Berkman Klein Center for Internet & Society Research, online: <https://dash.harvard.edu/bitstream/handle/1/28566279/SSRN-id2733350.pdf?sequence=1&isAllowed=y>.

La Presse Canadienne, "Logiciels espions : le commissaire à la vie privée veut des évaluations d'impact", (8 August 2022), online : *Radio-Canada* <https ://ici.radio-canada.ca/nouvelle/1904010/logiciels-espion-impact-commission-vie-privee>.

———, "L'usage de logiciels espions par la GRC sera examiné par un comité parlementaire", (26 July 2022), online : *Radio-Canada* <https ://ici.radio-canada.ca/nouvelle/1901122/grc-logiciels-espions-comite-parlementaire-vie-privee>.

Law Reform Commission of Canada*, Electronic surveillance*, Working paper – Law Reform Commission of Canada No. 47 (Ottawa: Law Reform Commission of Canada, 1984).

Lee, Micah, "Encrypting your laptop like you mean it", (27 April 2015), online: *The Intercept* <https://theintercept.com/2015/04/27/encrypting-laptop-like-mean/>.

Levenson, Michael, "51 Years Later, Coded Message Attributed to Zodiac Killer Has Been Solved, F.B.I. Says" *NY Times* (11 December 2020), online: <https://www.nytimes.com/2020/12/11/us/zodiac-killer-code-broken.html>.

Lewis, Sarah, "Perfect forward secrecy (PFS)", (September 2018), online: *TechTarget* <https://www.techtarget.com/whatis/definition/perfect-forward-secrecy>.

MacKay, Peter, "House of Commons Debates", (27 November 2013), online: *Parliament of Canada* <https://www.ourcommons.ca/Content/House/412/Debates/025/HAN025-E.PDF>.

Marczak, Bill et al, "FORCEDENTRY – NSO Group iMessage Zero-Click Exploit Captured in the Wild", (13 September 2021), online: *Citizen Lab* <https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/>.

Matheson, Andrew & John W Boscariol, "UK SFO unable to compel US company to produce documents held outside the UK", (20 April 2021), online: *McCarthy Tétrault* <https://www.mccarthy.ca/en/insights/articles/uk-sfo-unable-compel-us-company-produce-documents-held-outside-uk>.

McAfee, "What is Endpoint Encryption?", online: *McAfee* <https://www.mcafee.com/enterprise/en-ca/security-awareness/endpoint/what-is-endpoint-encryption.html#types>.

McKinney, India & Erica Portnoy, "Apple's Plan to 'Think Different' About Encryption Opens a Backdoor to Your Private Life", (5 August 2021), online: *Electronic Frontier Foundation* <https://www.eff.org/deeplinks/2021/08/apples-plan-think-different-about-encryption-opens-backdoor-your-private-life>.

Menn, Joseph, "Dozens of Thai activists and supporters hacked by NSO Group's Pegasus", (17 July 2022), online: *Washington Post* <https://www.washingtonpost.com/technology/2022/07/17/pegasus-nso-thailand-apple/>.

Merriam-Webster, "Algorithm", online: <https://www.merriam-webster.com/dictionary/algorithm>.

Miller, Joe, "Google and Apple to introduce default encryption", (19 September 2014), online: *BBC* <https://www.bbc.com/news/technology-29276955>.

Montgomery, Kevin, "Proxy Services Are Not Safe. Try These Alternatives", (6 July 2015), online: *Wired* <https://www.wired.com/2015/07/proxy-services-totally-unsecure-alternatives/>.

Mozy, "Privacy Statement", online: *Mozy* <https://mozy.com/about/legal/privacy>.

Mullin, Joe, "The U.K. Paid $724,000 For A Creepy Campaign to Convince People That Encryption is Bad. It Won't Work.", (21 January 2022), online: *Electronic Frontier Foundation* <https://www.eff.org/deeplinks/2022/01/uk-paid-724000-creepy-campaign-convince-people-encryption-bad-it-wont-work>.

National Institute of Standards and Technology, "Advanced Encryption Standard (AES)", (26 November 2001), online: *NIST* <https://www.nist.gov/publications/advanced-encryption-standard-aes>.

National Institute of Standards and Technology, "Internet of Things (IoT)", online: *NIST* <https://csrc.nist.gov/glossary/term/internet_of_things_IoT>.

Nakashima, Ellen, "Apple vows to resist FBI demand to crack iPhone linked to San Bernardino attacks", *Wash Post* (17 February 2016), online: <https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html?itid=lk_inline_manual_8>.

Nakashima, Ellen & Reed Albergotti, "The FBI wanted to unlock the San Bernardino shooter's iPhone. It turned to a little-known Australian firm.", *Washington Post* (14 April 2021), online: <https://www.washingtonpost.com/technology/2021/04/14/azimuth-san-bernardino-apple-iphone-fbi/>.

Naudie, Christopher & John Cotter, "Enquêtes transfrontalières : la Cour d'appel de la Colombie-Britannique affirme son vaste pouvoir de lancer un processus judiciaire contre des sociétés étrangères", (18 December 2018), online : *Osler* <https ://www.osler.com/fr/ressources/transfrontaliers/2018/enquetes-transfrontalieres-la-cour-d-appel-de-la-colombie-britannique-affirme-son-vaste-pouvoir-de>.

Newman, Lily Hay, "End-to-End Encryption's Central Role in Modern Self-Defense", (5 July 2022), online: *Wired* <https://www.wired.com/story/end-to-end-encryption-abortion-privacy/>.

———, "The Apple-FBI Fight Is Different From the Last One", (16 January 2020), online: *Wired* <https://www.wired.com/story/apple-fbi-iphone-encryption-pensacola/>.

Nield, David, "How to Get the Most Out of Your Smartphone's Encryption", (29 January 2020), online: *Wired* <https://www.wired.com/story/smartphone-encryption-apps/>.

NordPass, "Top 200 most common passwords", (2022), online: *NordPass* <https://nordpass.com/most-common-passwords-list/>.

Organization for Economic Co-operation and Development, "Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data", online: *OECD* <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188>.

Ouimet, Roger, *Towards Unity: Criminal Justice and Corrections*, by Roger Ouimet (Ottawa: Canadian Committee on Correction, 1969).

Parliament of Australia, "Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 – Revised Explanatory Memorandum" (2018).

Parsons, Christopher, "Canada's New and Irresponsible Encryption Policy – How the Government of Canada's New Policy Threatens Charter Rights, Cybersecurity, Economic Growth, and Foreign Policy", (21 August 2019), online: *Citizen Lab* <https://citizenlab.ca/2019/08/canadas-new-and-irresponsible-encryption-policy-how-the-government-of-canadas-new-policy-threatens-charter-rights-cybersecurity-economic-growth-and-foreign-policy/>.

———, *The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians*, (Toronto: Telecom Transparency Project, 2015).

Parsons, Christopher & Tamir Israel, "Canada's Quiet History of Weakening Communications Encryption", (11 August 2015), online: *Citizen Lab*

<https://citizenlab.ca/2015/08/canadas-quiet-history-of-weakening-communications-encryption/>.

Payments Journal, "By 2024, How Many Smartphone Owners Will Use Biometrics?", (4 June 2020), online: *Payments Journal* <https://www.paymentsjournal.com/by-2024-how-many-smartphone-owners-will-use-biometrics/>.

Pearson, Jordan & Justin Ling, "Exclusive: How Canadian Police Intercept and Read Encrypted BlackBerry Messages – VICE", (14 April 2016), online: *Vice* <https://www.vice.com/en_us/article/mg77vv/rcmp-blackberry-project-clemenza-global-encryption-key-canada>.

Penney, Steven, "'To Catch a Predator': Reasonable Expectation of Privacy in R v Mills", (23 April 2019), online: *University of Alberta Faculty of Law* <https://ualbertalaw.typepad.com/faculty/2019/04/to-catch-a-predator-reasonable-expectations-of-privacy-in-r-v-mills.html>.

Perry Barlow, John, "A Declaration of the Independence of Cyberspace", (8 February 1996), online: *Electronic Frontier Foundation* <https://www.eff.org/cyberspace-independence>.

Public Safety Canada, *National Security Consultations – What We Learned Report* (Ottawa, Canada: Public Safety Canada, 2017).

———, *2020 Annual Report on the Use of Electronic Surveillance* (Public Safety Canada, 2021), online: <https://publications.gc.ca/collections/collection_2022/sp-ps/PS1-1-2020-eng.pdf>.

Rafter, Dan, "What is the difference between black, white and gray hat hackers?", (25 February 2022), online: *Norton* <https://us.norton.com/internetsecurity-emerging-threats-black-white-and-gray-hat-hackers.html>.

Rivera, Andreas, "A Small Business Guide to Computer Encryption", (29 January 2019), online: *Business News Daily* <https://www.businessnewsdaily.com/9391-computer-encryption-guide.html>.

Rogaway, Phillip, *The Moral Character of Cryptographic Work* (Auckland, New Zealand, 2015), 2015 IACR Distinguished Lecture.

Rubenking, Neil J, "The Best Encryption Software for 2021", (19 October 2021), online: *PC Mag* <https://www.pcmag.com/picks/the-best-encryption-software>.

Schneier, Bruce, "The Eternal Value of Privacy", (18 May 2006), online: *Wired* <https://www.wired.com/2006/05/the-eternal-value-of-privacy/#:~:text=Privacy%20is%20an%20inherent%20human,%22Absolute%20power%20corrupts%20absolutely.%22>.

Schulz, Wolfgang & Joris Van Hoboken, *Human Rights and Encryption*, by Wolfgang Schulz & Joris Van Hoboken, Series on Internet Freedom (France: UNESCO, 2016).

Seglins, Dave, Robert Cribb & Chelsea Gomez, "Inside 10 cases where the RCMP hit a digital wall" (2016) CBC, online: <https://www.cbc.ca/news/investigates/police-power-privacy-rcmp-cases-1.3850783>.

———, "RCMP want new powers to bypass digital roadblocks in terrorism, major crime cases" (2016) CBC, online: <https://www.cbc.ca/news/investigates/rcmp-digital-roadblocks-1.3850018>.

Selyukh, Alina, "A Year After San Bernardino And Apple-FBI, Where Are We On Encryption?", (3 December 2016), online: *NPR.org* <https://www.npr.org/sections/alltechconsidered/2016/12/03/504130977/a-year-after-san-bernardino-and-apple-fbi-where-are-we-on-encryption>.

Silver, Lisa, "A Look Down the Road Taken by the Supreme Court of Canada in *R v Mills*", (8 May 2019), online: *University of Calgary Faculty of Law* <https://ablawg.ca/2019/05/08/a-look-down-the-road-taken-by-the-supreme-court-of-canada-in-r-v-mills/>.

Singel, Ryan, "Encrypted E-Mail Company Hushmail Spills to Feds", (11 July 2007), online: *Wired* <https://www.wired.com/2007/11/encrypted-e-mai/>.

Sirota, Leonid, "What was Equilibrium Like?", (31 May 2019), online: *Double Aspect* <https://doubleaspect.blog/2019/05/31/what-was-equilibrium-like/>.

Sottek, TC & Janus Kopfstein, "Everything you need to know about PRISM", (17 July 2013), online: *The Verge* <https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet>.

Sparrow, Andrew, "No 10 revives prospect of UK leaving European convention on human rights after Labour calls Rwanda plans 'a shambles' – as it happened", (15 June 2022), online: *The Guardian* <https://www.theguardian.com/politics/live/2022/jun/15/rwanda-flight-asylum-echr-priti-patel-boris-johnson-pmqs-uk-politics-latest>.

SpiderOak, "No Knowledge, Secure-by-Default Products", online: <https://spideroak.com/no-knowledge/>.

———, "Privacy Policy", online: *SpiderOak* <https://spideroak.com/privacy-policy/>.

Standing Senate Committee on Legal and Constitutional Affairs*, Proceedings of the Standing Senate Committee on Legal and Constitutional Affairs, No. 44, 3rd Sess.* (Standing Senate Committee on Legal and Constitutional Affairs, 34th Parl., 1993).

Standing Committee on Public Safety and National Security*, Cybersecurity in the Financial Sector as a National Security Issue* (Ottawa, Canada: Standing Committee on Public Safety and National Security, 2019).

Sandvine, "The Global Internet Phenomena Report – October 2018", (2018), online: *Sandvine* <https://www.sandvine.com/hubfs/downloads/phenomena/2018-phenomena-report.pdf>.

Statewatch, “EU: End game approaching for e-evidence negotiations, says French Presidency”, (6 July 2022), online: *Statewatch* <https://www.statewatch.org/news/2022/july/eu-end-game-approaching-for-e-evidence-negotiations-says-french-presidency/>.

Statistics Canada, “Police-reported cybercrime, number of incidents and rate per 100,000 population, Canada, provinces, territories, Census Metropolitan Areas and Canadian Forces Military Police”, (2 August 2022), online: *Statistics Canada* <https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=3510000201>.

Stilgherrian, *The Encryption Debate in Australia: 2021 Update*, (Washington, DC: Carnegie Endowment for International Peace, 2021).

Stokel-Walker, Chris, “Data Centers Are Facing a Climate Crisis”, (1 August 2022), online: *Wired* <https://www.wired.com/story/data-centers-climate-change/>.

Symanovitch, Steve, “The Future of IoT: 10 Predictions about the Internet of Things”, (2019), online: *Nort Symantec* <https://us.norton.com/internetsecurity-iot-5-predictions-for-the-future-of-iot.html>.

TechTarget, “full-disk encryption (FDE)”, (December 2014), online: *What Is* <https://whatis.techtarget.com/definition/full-disk-encryption-FDE>.

———, “Public Key”, (June 2021), online: *TechTarget*, <https://www.techtarget.com/searchsecurity/definition/public-key#:~:text=The%20key%20can%20be%20generated,legitimacy%20of%20a%20digital%20signature.>.

TechTerms, “Authentication”, (2018), online: *TechTerms* <https://techterms.com/definition/authentication>.

Therrien, Daniel, “Bill C-13, the Protecting Canadians from Online Crime Act – Submission to the Standing Senate Committee on Legal and Constitutional Affairs”, (19 November 2014), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2014/parl_sub_141119/>.

Timberg, Craig, “Apple will no longer unlock iPhones for police”, (18 September 2014), online: *Police1* <https://www.police1.com/legal/articles/apple-will-no-longer-unlock-iphones-for-police-pJmeWqziSHVBN4AP/>.

Timberg, Craig, Drew Harwell & Ellen Nakashima, “NSO Pegasus spyware used to hack U.S. diplomats working abroad”, (3 December 2021), online: *Washington Post* <https://www.washingtonpost.com/technology/2021/12/03/israel-nso-pegasus-hack-us-diplomats/>.

United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, A/HRC/39/29 (2018).

United Nations – Office on Drugs and Crime, "Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes", online: *UNODC* <https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home>.

United Kingdom's Attorney General's Office*, Joint Meeting of Five Country Ministerial and quintet of Attorneys-General: communiqué, London 2019 (accessible version)* (United Kingdom: UK's Attorney General's Office, 2019).

United Kingdom's Supreme Court, "The Supreme Court and Europe – What is the relationship between the UK Supreme Court, the European Court of Human Rights, and the Court of Justice of the European Union?", (2022), online: *Supreme Court* <https://www.supremecourt.uk/about/the-supreme-court-and-europe.html>.

Vera Crypt, "Hidden Volume", online: *Vera Crypt* <https://veracrypt.eu/en/docs/hidden-volume/>.

WhatsApp, "WhatsApp Security", online: *WhatsApp.com* <https://www.whatsapp.com/security/>.

Williams, George, "The Federal Parliament and the Protection of Human Rights", (1999), online: <https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp9899/99rp20>.

Zittrain, Jonathan L et al, *Don't Panic: Making Progress on the "Going Dark" Debate* (The Berkman Center for Internet & Society at Harvard University, 2016).

Secondary Materials: Others

Geist, Michael, *David Fraser on Negotiating a CLOUD Act Agreement Between Canada and the United States*, Law Bytes Podcast, online: <https://www.michaelgeist.ca/2022/04/law-bytes-podcast-episode-124/>.

The Da Vinci Code (Sony Pictures, 2006).