Smart Devices in Criminal Investigations: How Section 8 of the *Canadian Charter of Rights and Freedoms* can better Protect Privacy in the Search of Technology and Seizure of Information

By

Lee-Ann Verna Conrod

Submitted in partial fulfilment of the requirements
for the degree of Master of Laws

at

Dalhousie University
Halifax, Nova Scotia
August 2018

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

First and foremost, I praise God, who is infinitely able, for providing me this opportunity and giving me the purposeful desire to succeed.

I must express my very profound gratitude to my parents Mona Bonnyman and Allan Conrod, my step-mother Pam Sherren, and my Grammie Dorothy Conrod, for providing me with unfailing support and continuous encouragement throughout the process of researching and writing this thesis. I would also like to thank my sister, Kristen Conrod, for always believing in me and cheering me on. This accomplishment would not have been possible without their unconditional love.

Thank you.

ABSTRACT

This thesis examines the jurisprudence from the Supreme Court of Canada (SCC) on informational privacy under section 8 of the *Canadian Charter of Rights and Freedoms* as it relates to searches of technology in the context of criminal investigations. The development and use of technology in criminal investigations will be detailed along with an overview of the current state of the law in this area. Challenges with the interpretation of section 8 demonstrate a prevalent uncertainty. This thesis proposes a new approach for the SCC to apply to cases where technology intersects with section 8 of the *Charter*. The proposal rests on a clearer and broader understanding of privacy along with measurable categories for more predictable outcomes.

CHAPTER 1: INTRODUCTION

Law enforcement in Canada are tasked with preventing and investigating crime.[1] To investigate crime, police regularly use a variety of tools including the common practices of conducting physical surveillance and gathering intelligence from confidential informants. The use of technology in criminal investigations is a relatively new and quickly developing phenomenon. In some cases, technology is employed by criminals specifically to avoid police detection. The use of cryptocurrencies to hide the profits of crime and anonymous online websites or services to conduct criminal transactions are examples of this. More commonly, technology is a collateral part of a criminal investigation. For example, because of technological developments child pornography is now accessible through the internet. Drug and weapons trafficking arrangements are made via text messages on smart phones. Today more crimes are inadvertently leaving behind digital data in the form of IP addresses, search history or electronic records of the criminal activities. In the same way technology provides criminals with the means and method to commit crimes, it can provide vast amounts of specific and accurate information about their activities that would assist law enforcement in their investigations.

Law enforcement would like to have access to this digital evidence in every case but there are restrictions to their ability to search for and seize it. This limitation to police powers is expressed in section 8 of the *Canadian Charter of Rights and Freedoms*, which provides that "Everyone has the right to be secure against unreasonable search or seizure."[2] Section 8 is used to determine whether a search and/or seizure is lawful. To investigate and prosecute an accused

[1] See for example RCMP, "About the RCMP" (May 7, 2018) online: http://www.rcmp-grc.gc.ca/about-ausujet/index-eng.htm.
[2] *Canadian Charter of Rights and Freedoms,* Part I of the *Constitution Act, 1982*, Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11 [*Charter*].

person with the aim of achieving a conviction, the police must have gathered the evidence lawfully so that it is admissible at trial.

While the provision of section 8 itself is straightforward, the jurisprudence is not. The Supreme Court of Canada (SCC) has dealt with the intersection of informational privacy and technology on a variety of occasions over the past three decades. Accused persons have argued before the SCC that they have had their right to privacy violated with respect to their movements captured by a tracking device[3], electricity consumption records obtained from a utility company[4], heat patterns in their home viewed through forward looking infrared technology[5], child pornography files on their home computer[6] and work laptop[7], and incriminating text messages conversations.[8] The Court has provided general principles to assist in the interpretation of section 8, specifically that it should be governed by a flexible and normative analysis.[9] The Court has identified the purpose of section 8 as to prevent unjustified state intrusion on individual privacy.[10] They have created a variety of tools of analysis to achieve this purpose including the totality of the circumstances test and the concept of a biographical core of information. Yet, the jurisprudence from the SCC has not provided the desired certainty or predictability. Split decisions, caveats and an ad hoc approach create confusion that leaves justice participants guessing where the Court will fall on developing issues with emerging technology.

---

[3] *R v Wise*, [1992] 1 SCR 527, 11 CR (4th) 253 [*Wise*].
[4] *R v Plant*, [1993] 3 SCR 281, 24 CR (4th) 47 [*Plant*]; *R v Gomboc*, 2010 SCC 55, [2010] 3 SCR 211 [*Gomboc*].
[5] *R v Tessling*, 2004 SCC 67, [2004] 3 SCR 432 [*Tessling*].
[6] *R v Morelli*, 2010 SCC 8, [2010] 1 SCR 253 [*Morelli*].
[7] *R v Cole*, 2012 SCC 53, [2012] 3 SCR 34 [*Cole*].
[8] *R v Fearon,* 2014 SCC 77, [2014] 3 SCR 621 [*Fearon*]; *R v Marakah*, 2017 SCC 59, [2017] 2 SCR 608 [*Marakah*]; *R v Jones*, 2017 SCC 60, [2017] 2 SCR 696 [*Jones*].
[9] *Canada (Director of Investigation & Research, Combines Investigation Branch) v Southam Inc*., [1984] 2 SCR 145, 11 DLR (4th) 641 [*Hunter v Southam*], paras 16, 18-19 and 26; see also Don Stuart, *Charter Justice in Canadian Criminal Law*, 6th ed. (Toronto: Carswell, 2014) [Stuart], page 290.
[10] *Hunter v Southam*, paras 25 and 27.

The practical problems at the root of the section 8 analysis can be seen in the recent case of *R v Mills*.[11] In *Mills*, a police officer created a fictitious Facebook profile appearing as a 14-year-old girl, "Leann Power". Over the course of two months Sean Mills, a 31-year old man, communicated with Leann through thousands of messages on the social media platform, some being overly sexual in nature, which police captured using an online tool called Snag-It.[12] Mills was charged with four counts of child luring contrary to the *Criminal Code*.[13] Mills alleged that the search was an unreasonable violation of his privacy.[14] The Crown said it was not and sought to use the messages seized from Facebook as evidence to secure his conviction. This case involved technology being used in the commission of the crime and raises the question of when and how technology can be used by the police to investigate crime and when they can lawfully seize the digital evidence.

Mills is not an isolated case. Police are constantly faced with technological opportunities that would significantly assist in their investigations. For example, if police know that a suspect regularly wears a smart watch, Fitbit or owns a cellphone they know that there is data available about that person's exact whereabouts. If the suspect has smart devices in their home, such as a smart fridge, security system or lightbulb, that data can be used to gather intelligence on the person's activities. For those who own a digital assistant, such as an Alexa or Echo, they actually own a listening device that police could certainly use to gather information about the person's life. One would assume that people expect privacy in these devices and their information will be reasonably protected from police access.

[11] *R v Mills*, 2017 NLCA 12, [2017] 136 WCB (2d) 728 [*Mills*], leave to appeal of SCC granted.
[12] *Mills*, SCC Factum of HMTQ, paras 13, 24 and 25.
[13] *Criminal Code*, RSC 1985, c C-46 [*Criminal Code*], section 172.1(1).
[14] *Mills*, SCC Factum of Sean Patrick Mills, para 1.

Protecting an individual's privacy in technology from the State in the context of a criminal investigation is complex. The central focus of this thesis is to answer the question: in the context of criminal investigations, how can the line be drawn between lawful and unlawful searches of technology in light of the jurisprudence on section 8 of the *Charter*? And, given the challenges with the current jurisprudence, how should the law be modified to bring greater legal certainty?

1.1 METHODOLOGY

This thesis attempts to answer these questions using three approaches to legal analysis, namely the doctrinal, historical and interdisciplinary methods.

Doctrinal

To understand informational privacy in the context of technology, I will review the case law, legislation and arguments presented within section 8 litigation. This will be done using the doctrinal method. The doctrinal method involves the analysis of existing legal doctrine through a review of cases, statutes, rules and literature.[15] Doctrinal research provides the means to describe the legal context for this project and frame the issues surrounding informational privacy. Since informational privacy is located within *Charter* jurisprudence, the *Charter* and case law from the Supreme Court of Canada interpreting and applying section 8 will be a primary focus of this project, specifically in chapters 3 and 4. Traditional texts, such as the *Criminal Code* and academic writings will of course be reviewed. I will also canvass online blogs, news and main stream media

[15] Terry Hutchinson and Nigel Duncan, "Defining and Describing What We Do: Doctrinal Legal Research" (2012) 17 Deakin LR 83.

writings to gain a wider range of perspectives. Foundational principles revealed from a doctrinal review will be used in chapter 5 to build upon and frame a proposed new approach to section 8.

Historical

The historical method is concerned with tracing the history of a particular development within the law and possibly as well its relationship to the history of society.[16] Historical method finds the context of texts.[17] Ideas rejected in the past may be relevant now and can perhaps be used in today's different set of circumstances.[18] I will use a primarily internal legal history approach, which is essentially historical doctrinal work.[19] In reviewing the judgements from the SCC, there are certainly ideas that were once prominent which have seemingly lost their importance.[20] I will use the historical method to set the stage for the reader and aim to learn lessons from the past.

Within the case law, it is important to review the positions of the parties and the interveners along with examining the judgments of the SCC in order to appreciate the significant differences in the approaches to the issues and articulation of the potential impact of the Court's decision. Their viewpoints are influential to the judgments and demonstrate the fundamental divide on the larger issue of online privacy. This internal history places the judgements in context to understand

[16] Robert Cryer, et al. *Research Methodologies in EU and International Law* (Oxford: Hart Publishing, 2011) [Cryer], page 88.
[17] *Ibid*.
[18] *Ibid*. See also Jim Phillips, "Why Legal History Matters" (2010) 41 VUWLR 293.
[19] As opposed to external legal history which looks at context and sources outside the law.
[20] For example, the idea that informational privacy protected the "biographical core" of individual's information was a staple of section 8 cases in the 1990s and early 2000s but has since seen a decline in its importance and relevance to SCC's decision making. See Chris Hunt and Micah Rankin, "*R. v. Spencer*: Anonymity, The Rule of Law, and the Shriveling of the Biographical Core" (2015) 61 McGill L J 193 ["Shriveling of the Biographical Core"].

the legal landscape so that one can appropriately analyze the development of informational privacy protections.

External historical method will be used in this project to study how privacy law has developed since the *Charter*'s implementation and how technology has developed since the advent of the internet. This is done to establish the "historico-political context" for legal arguments and provide the "backdrop to judicial decisions".[21]

While history will be relevant to framing this research by appreciating where the law is today, I do not intend to focus on the history of section 8 of the *Charter* as the main theme for this project. History is able to answer some questions, primarily contextual, but is limited in its ability to address the forward looking and present problem of police searches of technology.

Interdisciplinary

Legal problems are in fact social, economic, political problems. Legal questions cannot always be answered through the law alone.[22] One type of interdisciplinary work is empirical. Statistics can be used to get a holistic view of the field of law as part of a wider context.[23] I will be referring to statistics in this project to demonstrate the size of the issue.[24] With the use of social media, the internet and the growing Internet of Things (IoTs), it will be useful to understand the scope of the issue and the number of people directly affected by this project. To do this, I draw

[21] Cryer, page 88.
[22] Moti Nissani, "Ten Cheers for Interdisciplinarity: The Case for Interdisciplinary Knowledge and Research (1997) 34 Soc Sci J 201.
[23] Cryer, pages 76-78.
[24] For example, the number of Facebook users, Twitter accounts, Alexa's sold in Canada, etc.

upon empirical evidence to demonstrate the problem – i.e. billions of Facebook users, profits realized by technology companies[25] – which cannot be explored solely within the field of law.

1.2 THESIS LAYOUT

First this thesis examines how technology has become a valuable and desirable component of many criminal investigations. I provide a brief history of technology then address the reality of mass data collection and data breaches. I detail how technology acts as a scrupulous record keeper and how all this data can be beneficial to police. I also discuss the potential for social media and the IoTs to collect and provide relevant information. Technology captures incriminating information automatically, as a consequence of the use of an online service or device, but it can also be used intentionally as a tool for committing crime. I provide examples of how technology is used and how it is relevant to criminal investigations.

Chapter 3 outlines the development and current state of the law on section 8 of the *Charter*. The SCC has interpreted section 8 of the *Charter* as requiring a normative inquiry, focusing on the concept of a reasonable expectation of privacy. Early jurisprudence established that the task of any section 8 analysis is to balance individual privacy interests with law enforcement efforts.[26] This chapter introduces the reader to the sphere of informational privacy as articulated by the SCC and two tools of analysis employed by the Court in these section 8 cases. In reviewing the tools

[25] See David Kirkpatrick, *The Facebook Effect: The Inside Story of the Company that is Connecting the World* (Toronto: Simon & Schuster, 2010) [*The Facebook Effect*]; Siva Vaidhyanathan, *The Googlization of Everything (And Why We Should Worry)* (Los Angeles: University of California Press, 2011) [*The Googlization of Everything*]; Lori Andrews, *I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy* (New York: Free Press, 2012) [*Social Networks and the Death of Privacy*].
[26] *Hunter v Southam*, para 25.

of analysis – biographical core and totality of the circumstances – it becomes clear that there are serious deficiencies in their ability to deal with search and seizure issues in the context of technology.

Chapters 2 and 3 together provide the necessary background to answer the question of how the line can be drawn between lawful and unlawful searches of technology and whether the current framing of section 8 needs to be adjusted to adequately deal with current technology search issues.

In chapter 4, I assess the effectiveness of the framework currently in place and explore contextual factors around the interpretation of section 8 with a view to examining the major challenges to achieving certainty. This chapter focuses on the Court's purported normative approach and how that approach is not compatible with the tools of analysis designed by the Court. I also outline a variety of ways in which the Court has added to the uncertainty in their jurisprudence through their judgements. Lastly, this chapter briefly addresses how the problems with searches of technology are compounded by the relevant legislation. Essentially, this chapter establishes the absence of an authoritative answer to my research question.

Chapter 5 recommends a way forward for the SCC to better address searches of technology within section 8 parameters. I propose a new framework for the analysis of section 8 which includes expanding section 8 *Charter* protection past individual considerations of privacy to a collective understanding of the right which includes using a spectrum of protection. That spectrum would be assessed using four criteria: intrusiveness, specificity and accuracy of the search and the type of detail revealed. Three categories along the spectrum are described which demonstrate the usefulness of this approach. Chapter 6 concludes this thesis with a view to bringing greater legal certainty to section 8 of the *Charter* in the context of technology in criminal investigations.

CHAPTER 2: THE USE OF TECHNOLOGIES IN CRIMINAL INVESTIGATIONS

2.1 INTRODUCTION

This chapter looks at the current state of technology in our society to better understand how it has become a valuable and desirable component of many criminal investigations. I first detail a brief history of technology in section 2.2 then address the reality of mass data collection and its insecurity in section 2.3. I discuss our culture of accepting surveillance in section 2.4, other trends in social media in section 2.5 and the Internet of Things (IoTs) in section 2.6. Each of these sections contributes to our understanding of how technology is part of criminal investigations. Section 2.7 details how technology can be used as a tool for committing crime and avoiding law enforcement. Lastly, section 2.8 draws out the implications of technology for criminal investigations. The question to consider is how adequately the SCC's current jurisprudence on section 8 of the *Charter* deals with the developing technological challenges and their privacy implications.

2.2 A BRIEF HISTORY OF TECHNOLOGY

Technology is ever evolving, and the use of technology has grown exponentially since the implementation of the *Charter* in 1982 and the first consideration of section 8 in *Hunter v Southam* in 1984. To understand the current state of affairs, it is useful to briefly explore the history of the internet and how rapidly technology has developed.

The history of computers and the internet is actually less than 50 years old. The personal computer was developed in the 1970s[27] and in 1979 a protocol was created that allowed computers

[27] Reg Whitaker, *The End of Privacy: How Total Surveillance is Becoming a Reality* (New York: The New Press, 1999) [*The End of Privacy*], page 54.

to link together over the telephone which "grew together into a network of all networks, the internet".[28] At that time, no one imagined today's network connecting hundreds of millions of computers around the globe. It was in 1978 that the first satellites were launched for the Global Positioning System (GPS).[29] In the 1990s, email began to be used by the general public.[30] In 1996 John Perry Barlow – a cattle rancher, lyricist for the Grateful Dead, founding member of the Electronic Frontier Foundation and a cyberlibertarian[31] – wrote "A Declaration of the Independence of Cyberspace" as part of a movement against the regulation of the internet.[32] At that time, cyberspace was thought of as a lawless world; somewhere you went to escape.[33] Today, that image is no longer accurate since we are almost constantly online and we can now stray onto the internet without knowing it.[34]

The internet, personal computers, cell phones, GPS and emails are now an ordinary part of everyday life in our society. Technology has changed everything – it has transformed and continues to transform our economy, society, culture and our understanding of human interaction.[35] The internet has been described as "one of the most important and powerful creations

---

[28] *The End of Privacy*, page 54. See also Jonathan Zittrain, *The Future of the Internet - and How to Stop It* (London: Yale University Press, 2008), page 36 for description of growth of internet.
[29] Viktor Mayer-Schonberger and Kenneth Cukier, *Big Data: A Revolution that will Transform how we Live, Work, and Think* (New York: Houghton Mifflin Harcourt Publishing Company, 2013) [*Big Data*], page 88.
[30] *The Facebook Effect*, page 67.
[31] The Guardian, "John Perry Barlow Obituary" (February 11, 2018) online: https://www.theguardian.com/technology/2018/feb/11/john-perry-barlow-obituary.
[32] John Perry Barlow, "A Declaration of the Independence of Cyberspace" (February 8, 1996) online: https://www.eff.org/cyberspace-independence.
[33] Robert Currie and Teresa Scassa, "New First Principles? Assessing the Internet's Challenges to Jurisdiction" (2011) 42 Geo J Intl L 1017 [New First Principles], page 1037.
[34] With our devices connected to the internet, we do not even know when we are crossing over into "cyberspace" and when we are not. We do not "go to" cyberspace, it is constantly interacting with us.
[35] *The End of Privacy*, page 47. See also *Morelli*, para 114 wherein Justice Deschamps states: "Internet and computer technologies have brought about tremendous changes in our lives. They facilitate the communication of information and the exchange of material of all kinds and forms, with both legal and illegal content, and in infinite quantities." para 114. See also Hal Abelson, et al, *Blown to Bits: Your Life, Liberty, and Happiness After the Digital Explosion* (Toronto: Addison-Wesley, 2008) [*Blown to Bits*], page 4 for discussion of digital explosion. In 2006, Time Magazine declared its Person of the Year to be "You" stating "You control the information age. Welcome to your world." Time

in all of human history".[36] It is hard to argue with that statement considering the impact the internet has had on our society – how we communicate, learn, interact with friends and go about our daily lives. In fact, access to the internet has transitioned from a luxury to a human right.[37]

Technology has become pervasive, omniscient, omnipotent and omnipresent. A discussion of the collection of our data will demonstrate this point.

2.3 MASS DATA COLLECTION AND ITS INSECURITY

The SCC's approach to informational privacy affects anyone with a credit card, rewards card, cell phone, smart device, vehicle, computer or social media profile. That is because we live in a monitored world of mass data collection; technology is pervasive and almost every aspect of our lives is connected.[38] It should not come as a surprise that more data is being collected, stored, shared and saved about us than ever before,[39] and that an ordinary person now generates a colossal amount of digital information.[40] Entire books are written about mass data collection.[41] We are

---

Magazine, "Person of the Year" (December 25, 2006) online: http://content.time.com/time/covers/0,16641,20061225,00.html.

[36] Dave Evans, "The Internet of Things: How the Next Evolution of the Internet is Changing Everything" (CISCO Internet Business Solutions Group, 2011) [CISCO Report], online: www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf, page 2. See also The Economist, "Plant of the Phones" (February 26, 2015) online: https://www.economist.com/news/leaders/21645180-smartphone-ubiquitous-addictive-and-transformative-planet-phones for how the smart phone has changed society.

[37] See New First Principles, page 1044-45 for discussion of internet access as a human right. See also CBC, "CRTC Declares Broadband Internet Access a Basic Service" (December 21, 2016) online: http://www.cbc.ca/news/politics/crtc-internet-essential-service-1.3906664, Jean-Pierre Blais, CRTC's Chair stated that the internet is a vital service, essential to life and success. And see Wired, "UN Report Declares Internet Access a Human Right" (June 3, 2011) online: https://www.wired.com/2011/06/internet-a-human-right/.

[38] See Kieron O'Hara and Nigel Shadbolt, *The Spy in the Coffee Machine: The End of Privacy as we Know It* (Oxford: One World Publications, 2008) [*The Spy in the Coffee Machine*], page 26 for discussion of "fully fledged surveillance societies" where "most people live reasonably and happily with surveillance".

[39] *Big Data*, page 150.

[40] *The Spy in the Coffee Machine*, page 98.

[41] See for example, Robert Vamosi, *When Gadgets Betray Us: The Dark Side of our Infatuation with New Technologies* (New York: Basic Books, 2011); *Big Data*; Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your*

under constant digital surveillance. Rewards cards, credit cards and banking cards offer rewards and convenience in exchange for our data.[42] They are effectively electronic tags that locate and track individuals' habits.[43] Our cell phones and smart watches and Fitbits track our every move. As Bruce Schneier, internationally renowned security technologist and Chief Technology Officer at IBM, explained:

> Your cell phone tracks where you live and where you work. It tracks where you like to spend your weekends and evenings. It tracks how often you go to church (and which church), how much time you spend in a bar, and whether you speed when you drive. It tracks – since it knows about all the other phones in your area – whom you spend your days with, whom you meet for lunch, and whom you sleep with. The accumulated data can probably paint a better picture of how you spend your time than you can, because it doesn't have to rely on human memory.[44]

Corporations use that information to find patterns of where individuals visit so they can employ targeted specific marketing.[45] Our internet activities leave a trail of information about what websites we visit, searches we conduct and our lifestyle choices.[46] Every time we like, follow, share or click we are producing data. For example, if a woman searches online for anything related to pregnancy, she is immediately identified and within seconds will be bombarded with advertisements for baby clothes, strollers, vitamins and pregnancy related items.[47] Internet Service Providers (ISPs) retain data that is regularly traded for targeted marketing of products and

---

Data and Control Your World (New York: WW Norton & Company, 2015) [*Data and Goliath*]; *The Googlization of Everything*.

[42] *Blown to Bits*, page 11 explains: "Such data is so valuable to planning the supply chain that stores will pay money to get more of it from their customers. That is really what supermarket loyalty cards provide – shoppers are supposed to think that the store is granting them a discount in appreciation for their steady business, but actually the store is paying them for information about their buying patterns. We might better think of a privacy tax – we pay the regular price unless we want to keep information about our food, alcohol, and pharmaceutical purchases from the market; to keep our habits to ourselves, we pay extra."

[43] *End of Privacy*, page 96. These cards capture every item purchased including date and time of purchase, the brand of every item, the exact time, store location and method of payment.

[44] *Data and Goliath*, page 1-2.

[45] See Jose Van Dijck, *The Culture of Connectivity: A Critical History of Social Media* (New York: Oxford University Press, 2013) [Culture of Connectivity], page 124 for discussion of how Google achieved the Holy Grail of monetizing strategies, "maximizing the ability to distribute personalized commercial messages to mass audiences".

[46] *Data and Goliath*; See also, *Big Data*.

[47] *Inside the Dark Web*, (BBC Worldwide Ltd., documentary film: 2014) [*Inside the Dark Web*].

services.[48] In most instances, we are unaware that the collection of data is even occurring since it is happening in the digital background.[49] All of that information could obviously be useful to law enforcement efforts to prevent and investigate crime.

The SCC has shown it is mindful of the magnitude of information that is collected through our digital activities. In 2014, Justice Karakatsanis acknowledged this phenomenon in the dissenting judgement of *Fearon*:

> The devices which give us this freedom also generate immense stores of data about our movements and our lives. Ever-improving GPS technology even allows these devices to track the locations of their owners. Private digital devices record not only our core biographical information but our conversations, photos, browsing interests, purchase records, and leisure pursuits. Our digital footprint is often enough to reconstruct the events of our lives, our relationships with others, our likes and dislikes, our fears, hopes, opinions, beliefs and ideas. Our digital devices are windows to our inner private lives.[50]

Electronic "bread crumbs" leave behind a trail that others can reconstruct years later.[51] While data collection is obviously valuable to corporations, law enforcement could also benefit significantly from having access to individuals' data. Police could easily find out the location of a suspect or patterns of a suspect's activities through searches of their technology.

The SCC has recognized that computers and cell phones are portals to a wealth of information which make them quantitatively and qualitatively different than other items.[52] *Morelli*

---

[48] Nathaniel Gleicher, "Neither a Customer Nor a Subscriber Be, Regulating the Release of User Information on the World Wide Web" (2008-09) 118 Yale LJ 1945, at 1948-1950; Hubbard, DeFreitas & Magotiaux, eds. "The Internet – Expectations of Privacy in a New Context" (2001-02) 45 Crim LQ 170, at 189-191. See also New First Principles, page 1062 for description of data retention developments for companies such as Google and Facebook.

[49] As explained in *Blown to Bits*, "It is almost as hard to avoid leaving digital footprints as it is to avoid touching the ground when we walk", page 28. See also *The Spy in the Coffee Machine* for discussion of privacy breaches occurring accidentally or unwittingly, page 73.

[50] *Fearon*, para 101.

[51] *The Spy in the Coffee Machine*, page 80.

[52] *Fearon*, para 125. See also Frank Addario and Andrew Burgess, "If You Don't Care about Privacy, Why Are You Wearing Pants?" (2015) 35:5 For the Defence – The Criminal Lawyers Association Newsletter ["If you Don't Care about Privacy"], for discussion of SCC's treatment of section 8 privacy cases.

was the first case wherein the SCC recognized the powerful privacy interests in digital data. Justice Fish said, "It is difficult to imagine a search more intrusive, extensive, or invasive of one's privacy than the search and seizure of a personal computer".[53] In *Vu*, the SCC explained that a search warrant for a home does not include searches of computers found inside. Justice Cromwell for the unanimous court explained:

> The privacy interests implicated by computer searches are markedly different from those at stake in searches of receptacles such as cupboards and filing cabinets. Computers potentially give police access to vast amounts of information that users cannot control, that they may not even be aware of or may have chosen to discard and which may not be, in any meaningful sense, located in the place of the search.[54]

For these reasons the SCC has consistently held that digital devices attract a high privacy interest.[55]

Data collection cannot be considered in isolation. We also need to consider what control we have over our enormous amount of electronic data. Technology, together with a connected world, means that we inevitably lose track of the digital information about us and retain little control over our information in the world.[56] Privacy policies that determine our ability to control our information are lengthy and complex, with consumers having no bargaining power and accepting the "click to accept" model of acquiescence. Consumers agree to terms without taking the time to understand what those terms mean.[57] In addition, many of the policies require working

---

[53] *Morelli*, para 2.
[54] *R v Vu*, 2013 SCC 60, [2013] 3 SCR 657 [*Vu*], para 24.
[55] See *Vu*, para 24; *Morelli*, paras 2 and 105; *Fearon*, para 197.
[56] *The Spy in the Coffee Machine*, page 210.
[57] See House of Commons, Report of the Standing Committee on Access to Information, Privacy and Ethics, *Privacy and Social Media in the Age of Big Data* (April 2013) from *Minutes of Procedings: Evidence*, 1st Session, 41st Parliament (June 12, 2012) 1230, page 14: "An average social media user would have to spend 20 hours a month to read to privacy policies that apply to Google and all the websites they visit. That is unfeasible. Saying that protection goes through information and consent is an illusion."

within privacy settings with a level of technical proficiency that many of us simply do not possess.[58]

Any discussion of mass data collection is not complete without addressing the reality of data breaches, hacks and security failures which have become an unfortunate side effect of technology and a normal part of our interaction with it. In 2014, CNN reported that 47% of American adults were hacked in that year.[59] According to their numbers, two of the largest hacks in 2014 were the 70 million Target customers' personal information and 33 million Adobe user's credentials that were compromised.[60] In 2016, Uber confirmed that a data breach affected 57 million of their customers and drivers[61], of which 815,000 were Canadians.[62] In 2017, Yahoo announced that 3 billion accounts – including email, Tumblr, Fantasy and Flickr – experienced a data breach in 2013.[63] One of the most widespread and well-known data breaches was the WannaCry ransomware outbreak from May 2017. The ransomware hit UK hospitals, forcing the closure of entire wards and the crippling of the National Health Service.[64] The WannaCry attack

---

[58] For example, according to The New York Times, Facebook's privacy policy has 50 settings with more than 170 options, see The New York Times, "Facebook Privacy: A Bewildering Tangle of Options" (May 12, 2010) online: https://archive.nytimes.com/www.nytimes.com/interactive/2010/05/12/business/facebook-privacy.html. See also *Social Networks and the Death of Privacy*, page 128-129 for discussion of privacy policies. The joke "why did Facebook go public? Because they couldn't figure out the privacy settings either" gained viral attention, see *Culture of Connectivity*, page 66 and Los Angeles Times, "Facebook: Reaction in the Twittersphere" (May 18, 2012) online: http://articles.latimes.com/ 2012/may/18/business/la-fi-tn-facebook-reaction-twitter-20120518.

[59] CNN, "Half of American Adults Hacked this Year" (May 28, 2014) online: http://money.cnn.com/ 2014/05/28/ technology/security/hack-data-breach/index.html.

[60] *Ibid.* See also CNN, "Target Hack is a Wake-Up Call on Privacy" (January 11, 2014) online: http://money.cnn.com/ 2014/01/11/technology/security/target-hack-privacy/index.html?iid=EL.

[61] BBC, "Uber Concealed Huge Data Breach" (November 22, 2017) online: www.bbc.com/news/technology-42075306.

[62] The Star, "Uber says 815,000 Canadians affected by Data Breach as Formal Investigation Opened" (December 11, 2017) online: https://www.thestar.com/business/2017/12/11/privacy-commissioner-to-investigate-uber-data-breach.html ["Uber says 815,000 Canadians affected"].

[63] CNN, "Every single Yahoo account was hacked – 3 billion in all" (October 4, 2017) online: http://money.cnn.com /2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html. See also, Wired, "Yahoo's 2013 email Hack actually Compromised Three Billion Accounts" (October 3, 2017) online: https://www.wired.com/ story/yahoo-breach-three-billion-accounts/.

[64] Forbes, "An NSA Cyber Weapon might be Behind a Massive Global Ransomware Outbreak" (May 12, 2017) online: https://www.forbes.com/sites/thomasbrewster/2017/05/12/nsa-exploit-used-by-wannacry-ransomware-in-

was described as a "cyber pandemic" as companies and governments were affected across the globe.[65] Tens of thousands of infections were reported in 74 countries as of May 12, 2017.[66] Also in 2017, Equifax announced a breach that involved sensitive data of 247 million consumers[67] and approximately 19,000 Canadians.[68] Equifax stated that personal information, including social security numbers were compromised.[69] The government of Canada has faced the threat and reality of cyberattacks.[70] In fact, the Globe and Mail reported that the federal government suffered 4,571 known "system compromises" in 2016.[71] More recently, Facebook "improperly shared" the data of up to 87 million of its users,[72] including more than 600,000 Canadians.[73] In a 2018 interview with CNBC, Jeff Faulkner, acting President and CEO of the National Foundation for Credit

---

global-explosion/#735792bde599. See also BBC News, "NHS cyber-attack: GPs and Hospitals hit by Ransomware" (May 13, 2017) online: www.bbc.com/news/health-39899646 ["NSH cyber-attack"].

[65] The Wall Street Journal, "More Cyberattack Victims Emerge as Agencies Search for Clues" (May 13, 2017) online: https://www.wsj.com/articles/more-cyberattack-victims-emerge-as-agencies-search-for-clues-1494671938.

[66] Wired, "The Ransomware Meltdown Experts Warned about is Here" (May 12, 2017) online: https://www.wired.com/2017/05/ransomware-meltdown-experts-warned/.

[67] The Globe and Mail, "Equifax Data Breach could become the Most Costly in Corporate History" (March 2, 2018) online: https://www.theglobeandmail.com/report-on-business/international-business/us-business/equifax-data-breach-could-become-the-most-costly-in-corporate-history/article38180834/. See also "Uber says 815,000 Canadians affected".

[68] The Star, "Equifax finds additional 2.4 Million in US impacted by 2017 Data Breach" (March 1, 2018) online: https://www.thestar.com/business/economy/2018/03/01/equifax-finds-additional-24-million-in-us-impacted-by-2017-data-breach.html.

[69] CNBC, "In the Wake of the Equifax Data Breach, Consumers More at Risk" (March 11, 2018) online: https://www.cnbc.com/2018/03/10/in-the-wake-of-the-equifax-data-breach-consumers-more-at-risk.html ["In the Wake of the Equifax Data Breach, Consumers More at Risk"].

[70] The Star, "StatsCan Hacked after Government Sites made Vulnerable: Officials" (March 13, 2017) online: https://www.thestar.com/news/canada/2017/03/13/statscan-hacked-after-government-sites-made-vulnerable-officials.html. CBC, "What You Need to Know about Canada Revenue Agency's 'Internet Vulnerability'" (March 14, 2017) online: www.cbc.ca/news/technology/canada-revenue-agency-cra-internet-vulnerability-bug-apache-struts-2-1.4023838. CBC, "State-sponsored Cyberattacks on Canada successful about Once a Week" (October 30, 2017) online: www.cbc.ca/news/politics/cyber-attacks-canada-cse-1.4378711. The Globe and Mail, "Hackers target Canadian Government's Energy and Resource Departments" (November 17, 2016) online: https://www.theglobeandmail.com/news/politics/hackers-target-governments-energy-and-resource-departments/article32890960/ [Hackers target Canadian Government's Energy and Resource Departments"].

[71] "Hackers target Canadian Government's Energy and Resource Departments". Public Safety Canada, *Horizontal Evaluation of Canada's Cyber Security Strategy – Final Report* (September 29, 2017).

[72] BBC, "Facebook Scandal 'hit 87 million users'" (April 4, 2018) online: www.bbc.com/news/technology-43649018.

[73] The Star, "More than 600,000 Canadians caught in Facebook Data Scandal" (April 4, 2018) online: https://www.thestar.com/news/canada/2018/04/04/more-than-600000-canadians-caught-in-facebook-data-scandal.html.

Counselling, stated that "there are roughly over 1,500 breaches a year".[74] It seems as though every year the data breaches and security failures are increasing in number and affecting more individuals.[75] Even Canadian banks are targets of hackers and cannot prevent data breaches of customers' personal data.[76] These breaches, obviously, vary in their severity based on the information that is stolen – ranging from passwords, date of birth and mother's maiden name to credit card and social insurance numbers.[77] There is now an entire industry based on cyber security.[78] It is important to note that a breach of privacy or hack of one company or individual is a breach of many people's privacy. The interconnectedness of technology and people within society through technology means that it is more likely a collective is impacted by any breach.

[74] "In the Wake of the Equifax Data Breach, Consumers More at Risk".

[75] Bloomberg, "2016 was a Record Year for Data Breaches" (January 19, 2017) online: https://www.bloomberg.com/news/articles/2017-01-19/data-breaches-hit-record-in-2016-as-dnc-wendy-s-co-hacked. See also NBC News, "More than 4 Billion Data Records were Stolen Globally in 2016" (January 30, 2017) online: https://www.nbcnews.com/storyline/hacking-in-america/more-4-billion-data-records-were-stolen-globally-2016-n714066. And see: Wired, "The Biggest Cybersecurity Disasters of 2017 So Far" (July 1, 2017) online: https://www.wired.com/story/2017-biggest-hacks-so-far/.

[76] For example, the Bank of Montreal and Simplii Financial, owned by CIBC were targeted by hackers: CBC, "Hackers Threaten to Reveal Personal Data of 90,000 Canadians caught in Bank Hack" (May 29, 2018) online: www.cbc.ca/news/business/bank-hack-tuesday-1.4682018.

[77] The Equifax breach involved a database that includes personal information including, "names, addresses and most crucially, data like social security numbers in the US or social insurance numbers in Canada." CBC, "Equifax Data Breach a 'Digital Disaster' for Canadians" (September 17, 2017) online: http://www.cbc.ca/news/canada/new-brunswick/nb-opinion-equifax-data-breach-1.4293609.

[78] See course offering from Harvard University, "Cybersecurity: Managing Risk in the Information Age", online: https://gs.harvardx.harvard.edu/harvard-cybersecurity-online-short-course-hm/?&ef_id=c:263435404471_d:c_n:g_ti:kwd-358401477327_p:_k:%2Bcyber%20%2Bsecurity_m:b_a:56898363791&gclid=EAIaIQobChMIq8Lb88jR2gIVBEsNCh0cuwyKEAMYASAAEgK8CvD_BwE; see also Vumetric, "Cyber Security for Industry 4.0" https://www.vumetric.com/en/industries/manufacturing/; and see Forbes, "What are the Biggest Challenges facing the Cybersecurity Industry?" (September 15, 2017) online: https://www.forbes.com/sites/quora/2017/09/15/what-are-the-biggest-challenges-facing-the-cybersecurity-industry/#4b41cbc72d62.

Popular culture has normalized data breaches and network hacks in fictional drama series. *CSI: Cyber*[79] and *Wisdom of the Crowd*[80] are two network television shows with hacking and technology as the main themes. In addition, other shows reference technology and data breaches regularly as part of their plot line.[81] It seems as though every network TV show has addressed hacking and data security breaches in at least one episode, reflecting our culture.

Several more pages could be written about data breaches, hacks and security failures. I think the point has been made – that we live in a society where it is more likely than not that you will experience some form of data breach, either with respect to your email, health records, banking or something more inconsequential. Data intrusions are now regular occurrences and no longer seem shocking.[82] In spite of these data breaches and security failures, individuals are still eager to

[79] CBS, "CSI Cyber" online: https://www.cbs.com/shows/csi-cyber/. Season 1: Episode 1 "Kidnapping 2.0" is about a case of hacked baby monitors used to kidnap an infant. Season 2: Episode 5 "Hack E.R." is about a hacker who takes control of a hospital's networked devices and threatens to kill a patient every hour. Season 2: Episode 14 "Fit-and-Run" follows the FBI team using a victim's fitness tracker to retrace her steps and solve her murder. While these plot lines may seem futuristic, each of these episodes and others reflect headline news stories and real events. Hacked baby monitors were in the news: CTV, "'Erie' Music, Man's Voice Creeps into Nursery after Baby Monitor Hacked" (July 23, 2015) online: https://www.ctvnews.ca/canada/eerie-music-man-s-voice-creeps-into-nursery-after-baby-monitor-hacked-1.2483170. See also Huffington Post, "Parental Warning: Your Baby Monitor can be Hacked" (August 24, 2017) online: https://www.huffingtonpost.com/healthline-/parental-warning-your-bab_ b_11668882.html. "Hack E.R." closely follows the events of WannaCry in the UK when a ransomware attacked the National Hospital Service. See also "NHS cyber-attack". See ABC, "Grey's Anatomy" online: http://abc.go.com/shows/greys-anatomy/episode-guide, this ABC TV show produced an episode wherein a hacker compromises the hospital's computer system for ransom money – Season 14: Episode 8 "Out of Nowhere". "Fit-and-Run" closely resembles these real life stories: CNN, "Cops Use Murdered Woman's Fitbit to Charge her Husband" (April 26, 2017) online: https://www.cnn.com/2017/04/25/us/fitbit-womans-death-investigation-trnd/index.html. See also, The Guardian, "Man Suspected in Wife's Murder after her Fitbit data Doesn't Match his Alibi" (April 25, 2017) online: https://www.the guardian.com/technology/2017/apr/25/fitbit-data-murder-suspect-richard-dabate.

[80] CBS, "Wisdom of the Crowd" online: https://www.cbs.com/shows/wisdom-of-the-crowd/. This drama is about a crowdsourcing crime-solving app and expert hackers.

[81] For example, *Bull* is a network TV show about a jury consultant who employs a hacker to "deep dive" into potential clients' and jurors' online activities, Global, "Bull" online: https://www.globaltv.com/bull/. On CTV, "Designated Survivor" online: https://www.ctv.ca/designated-survivor, Season 2: Episode 16 "Fallout" the entire Washington, DC power grid is shut down by a hacker. See also ABC, "Scandal" online: http://abc.go.com/shows/scandal/episode-guide, Season 7: Episodes 13, 14 and 15 feature a hack of the plane Air Force Two and the hacker's dark web activities. CBS, "Madam Secretary" online: https://www.cbs.com/shows/madam-secretary/episodes/215621/, Season 3: Episode 2 "The Linchpin" had an episode featuring the Secretary of State's residence being hacked wherein the McCord's household appliances go haywire.

[82] *Blown to Bits*, page 21.

obtain the newest technology. Opting out of social media and technology altogether is not a realistic option, unless you enjoy living like a hermit.[83] As one author explained: "it would mean opting out of sociality all together, since online activities are completely intertwined with offline social life".[84] This is the context and reality of technology today. Law enforcement are eager to gain access to criminal suspects' data in order to create a full picture of the individual's activity. Hacking into a computer device or gaining access through a security failure or benefiting from a data leak are ways for police to access that information but is any of those *lawful* access?

2.4 SURVEILLANCE AS ENTERTAINMENT

Willingly submitting to surveillance has become a trend within our mainstream entertainment. As Canadian communications theorist Marshall McLuhan claimed "the medium is the message" – meaning that the medium affects society in a fundamental way. His references were in relation to a change from print media to television, wherein television became the dominant medium and changed its users.[85] Popular culture has embraced the idea of Big Brother and surveillance as entertainment.[86] Voluntarily being under constant surveillance and having your

[83] See Elizabeth Paton-Simpson, "Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places" (2000) 50 Univ of Toronto LJ 305 ["Privacy and the Reasonable Paranoid"], page 305 for discussion of person named "Prudence" who "goes to extraordinary lengths to protect her privacy" by keeping her blinds drawn, refusing to talk to people on the phone, shreds her waste paper, develops all her own photographs, makes purchases using a pseudonym and PO box, etc.

[84] *Culture of Connectivity*, page 173.

[85] Historica Canada, "Heritage Minutes – Marshall McLuhan" online: https://www.historicacanada.ca/content/heritage-minutes/marshall-mcluhan. For discussion of McLuhan's theory and application to current dominant medium of internet see Richard Koch and Greg Lockwood, *Superconnect: The Power of Networks and the Strength of Weak Links* (London: Little, Brown, 2010), page 92-98.

[86] For discussion of surveillance space see John McGrath, *Loving Big Brother: Performance, Privacy and Surveillance Space* (New York: Routledge, 2004). McGrath's assertion is that the statement "you are under surveillance" is a "description of our culture", page 19. He argues that the "notion of privacy is functionally quite weak as a counter to the growth of surveillance", page 56. See also *Data and Goliath*, page 9 for description of "surveillance society". Television is another area of enormous growth, considering in the 1950s there was only a few channels and now there are more than 500, see *The End of Privacy*, page 145.

entire life open for viewing by the public has become a popular and desirable ambition.[87] For example, *Big Brother*, *Big Brother Canada* and *Celebrity Big Brother* are all popular Global TV shows based on 24-hour surveillance, called "live feeds".[88] Big Brother Canada's tag line at the end of every episode is "Remember, someone is always watching!". The *Survivor*[89] and *Real Housewives*[90] franchises are some of the most popular reality TV shows, along with an assortment of shows that follow the lives of different individuals – whether selling or renovating real estate,[91] cooking/baking,[92] finding a spouse,[93] or losing weight.[94] TV shows capturing the lives of individuals are very popular[95] with many of these shows having been on television for over a decade.[96] A more recent form of entertainment, YouTube, has allowed everyone and their dog to

[87] See *The Spy in the Coffee Machine*, page 20.
[88] See Global, "Big Brother" online: https://www.globaltv.com/bigbrother/. The website explains the concept of the show: "Big Brother follows a group of people living together in a house outfitted with dozens of high-definition cameras and microphones recording their every move, 24 hours a day. Each week, the Houseguests will vote someone out of the house. At the end, the last remaining Houseguest will receive a grand prize of $500,000". In the Canadian version, houseguests are competing for a prize of $100,000. See also CBC, "The Villain, the Faithful Romantic: Big Brother casting call Draws all Types" (September 23, 2017) online: http://www.cbc.ca/news/canada/saskatoon/villain-moral-centre-big-brother-6-saskatoon-1.4304427.
[89] CBS, "Survivor" online: https://www.cbs.com/shows/survivor/. *Survivor* is now in its 36th season.
[90] Bravo, "Real Housewives of Atlanta", "Real Housewives of Beverly Hills", "Real Housewives of New York", "Real Housewives of Orange County", "Real Housewives of Potomac", "Real Housewives of Vancouver", "Real Housewives of Toronto", plus spin-off show: "Vanderpump Rules", online: http://www.bravotv.com/.
[91] To name only a few: HGTV, "Property Brothers" online: http://www.hgtv.ca/shows/property-brothers/ and "Property Virgins" online: http://www.hgtv.ca/shows/property-virgins/ and "Love it Or List It Vancouver" online: www.hgtv.ca/shows/love-it-or-list-it-vancouver/. TLC, "Trading Spaces" online: https://www.tlc.com/tv-shows/trading-spaces/. Bravo, "Million Dollar Listing" online: http://www.bravotv.com/million-dollar-listing.
[92] There is an entire network dedicated to the reality TV of cooking or baking: Food Network, online: www.foodnetwork.ca/shows/, "Top Chef", "Iron Chef", "Chef School" and "Chopped" to name a few.
[93] TLC, "The Spouse House" online: https://www.tlc.com/tv-shows/the-spouse-house/. ABC, "The Bachelor", "The Bachelorette", "Bachelor in Paradise" online: http://abc.go.com/shows/the-bachelor. Also note, technology has turned match matching into an algorithm, see dating websites such as match.com and e-harmony.com.
[94] ABC, "Extreme Weight Loss" online: http://abc.go.com/shows/extreme-weight-loss, follows individuals for 365 days on their weight loss journey. TLC, "My 600 lb Life" online: https://www.tlc.com/tv-shows/my-600-lb-life/, follows people struggling with excessive weight through surgery and weight loss. See also, TLC, "Skin Tight" online: https://www.tlc.com/tv-shows/skin-tight/ and TLC, "Fat Chance" online: https://www.tlc.com/tv-shows/fat-chance/ that follow people through very personal weight loss experiences.
[95] Dr. Phil, "Dr. Phil" online: https://www.drphil.com/, is perhaps the pinnacle of oversharing on network television. Dr. Phil has made a career from sharing the intimate details of people's lives for entertainment. TLC has become synonymous with reality TV. TLC shows include: "90-day fiancé", "The Spouse House", "Sister Wives", "Say Yes to the Dress", "Kate plus Eight", "My Big Fat Fabulous Life", "My 600 lb Life", https://www.tlc.com/tv-shows/.
[96] For example: *The Bachelor's* first episode was in 2002 and is currently in its 22nd season; *Survivor* began in 2002 and is in its 36th season; Big Brother's first episode was in 2000 and is in its 19th season.

become an instant celebrity. YouTube's mission is "to give everyone a voice and show them the world".[97] It boasts over 1 billion users, with videos in 88 countries and 76 languages.[98] The company claims that 1 billion hours of video is viewed on a daily basis.[99] A popular trend on YouTube is now creating videos about YouTube videos, wherein people record their reactions and commentary on YouTube videos while they are watching them.[100] Many of us no longer *watch* television but have become the subject and entertainment through being *watched*. This form of entertainment illustrates how surveillance has become normalized and trivialized. As a society, we no longer fear George Orwell's *1984* description of Big Brother but have accepted, chosen and embraced surveillance.

Even if we are not the subject being watched on television or have our own YouTube channel, we still share details of our lives on Facebook, Twitter or other social media platforms. People describe their daily movements and activities, sometimes in excruciating detail, for their friends and acquaintances to follow. This cultural norm of sharing, and many times oversharing, provides law enforcement with information about our lives that we do not always appreciate.

2.5 USING SOCIAL MEDIA TO PERPETRATE AND INVESTIGATE CRIME

One cannot fully and accurately review the influence of technology in today's culture without mentioning social media. The norms for sociality have drastically changed for an entire

[97] YouTube, "About" online: https://www.youtube.com/yt/about/.
[98] YouTube, "For Press" online: https://www.youtube.com/intl/en/yt/about/press/.
[99] *Ibid*.
[100] These are called "reaction" videos. For example, you can watch YouTube, "YouTubers React to Top 10 Most Viewed YouTube Videos of All Time" online: https://www.youtube.com/watch?v=gcOQumLbvXI; a YouTube content creator watch and react to a cooking video: https://www.youtube.com/watch?v=OMeIMC_s0GQ; a doctor react to *Grey's Anatomy*: https://www.youtube.com/watch?v=-FyRzgJFeLE.

generation who understand social media as a normal part of our existence. The social impact of this form of media is immeasurable. Social media permeates our lives. Social media is internet based, interactive platforms that allow for multi-party live communication.[101] Facebook, Twitter, YouTube and many other social media platforms have created a "new reality" wherein people are connected on a global and instantaneous basis.[102] Facebook's mission is to "give people the power to build community and bring the world closer together".[103] Since its inception in 2004 as a university student project, Facebook has grown to 1.4 billion daily active users and 2.13 billion monthly active users as of December 2017.[104] Approximately 42% of Canada's entire population were Facebook users in 2010.[105] It is important to recognize that while Facebook has innumerable trivial messages and posts, it has also changed how "people communicate and interact, how markets sell products, how governments reach out to citizens, and even how companies operate. It is altering the character of political activism, and in some countries, it is starting to affect the process of democracy itself".[106] Facebook caused a shift in the boundaries of personal privacy with many users willingly displaying intimate details of their lives.[107]

The phrase "Facebook effect" has been coined to refer to the trend of ordinary individuals, with no specialized skills or training, initiating broadcast as editor, content creator, producer and distributor.[108] This is clearly seen through platforms like YouTube and Twitter. A popular micro-

[101] Stephen Coughlan and Robert Currie, "Social Media: The Law Simply Stated" 11 Can J L & Tech 229 [Social Media: The Law Simply Stated], page 230.
[102] Social Media: The Law Simply Stated, page 251.
[103] Facebook, "Newsroom" online: https://newsroom.fb.com/company-info/.
[104] *Ibid*. See also *The Facebook Effect* for details of Facebook's growth. For example, in November, 2004, just 10 months after it started, Facebook reached 1 million users. Ten months later, in October 2005 it had 5 million users, pages 103-151.
[105] *The Facebook Effect*, page 16.
[106] *The Facebook Effect*, page 15.
[107] *The Facebook Effect*, page 200-201 and see page 266 for discussion of how users volunteer vast amounts of data about themselves and generate more data through their behavior on the social media site.
[108] *The Facebook Effect*, page 8-9.

blogging platform, Twitter, allows users to communicate with 280 characters at a time.[109] In 2009, Twitter had 50 million members.[110] Twitter is now a "global format for online public commentary" and a common tool for cultural discourse.[111] Given its immediate and brief nature, Twitter has become embedded in society as a "stream of global consciousness" [112] allowing everyone to see what is "happening in the world right now".[113]

These platforms have been normalized into everyday life. They show an "acceptance of connective media penetrating all aspects of sociality".[114] Even our vocabulary has adjusted to this new social media world.[115] The word "tweet" was added to the Oxford English Dictionary in June 2013[116] and "unfriend" was named the "2009 Word of the Year" by Oxford Dictionaries.[117] TV shows imbed social media in their storylines and provide interactive opportunities throughout their broadcasting.[118] Social media has changed the way people communicate and our collective expectations of privacy in those communications. There has been a shift in what society consider private and personal versus public. Social media favours sociality, openness and sharing. In addition, there has been a dramatic change in the level of interconnectedness between people, where our networks no longer consist of just our relatives and close friends.

---

[109] Twitter, "How to Use Media Studio" online: https://help.twitter.com/en/using-twitter/media-studio. See also YouTube, "Twitter Explained" online: https://www.youtube.com/watch?v=RoHhNisGMk8. And see, Elizabeth Kirley, "Can Twitter and BlackBerry Keep a Secret?" RegQuest March, 2011.
[110] *The Facebook Effect*, page 311.
[111] *Culture of Connectivity*, page 76-77. Discussion of "enormous quantity" of tweets: daily number of tweets increased from 27 million in 2009 to 290 million in February 2012. This is astonishing growth, considering the first blog was written in 1997, see *The Spy in the Coffee Machine*, page 141.
[112] *Culture of Connectivity*, page 77.
[113] Twitter, "home page" online: https://twitter.com/?lang=en.
[114] *Culture of Connectivity*, page 129.
[115] *Culture of Connectivity*, page 69.
[116] Oxford English Dictionary, "A Heads Up for the June 2013 OED Release" online: https://public.oed.com/the-oed-today/recent-updates-to-the-oed/previous-updates/june-2013-update/a-heads-up-for-the-june-2013-oed-release/.
[117] Oxford Dictionaries, "Word of the Year 2009" online: https://en.oxforddictionaries.com/word-of-the-year/word-of-the-year-2009.
[118] See *The Facebook Effect*, page 334.

Social media is used as both a means for criminals to commit their crimes and as a way for law enforcement to investigate criminal activity. The frequency of online child exploitation has resulted in a specialized unit of the RCMP. The National Child Exploitation Coordination Centre deals exclusively with "investigations related to the sexual exploitation of children on the internet in Canada".[119] As the *Mills* case demonstrated, social media platforms like Facebook are used by predators to find and communicate with vulnerable children with the aim to sexually abuse them. *Mills* also shows how police can use social media to investigate and capture those predators. Law enforcement can observe our social media lives and engage with us through social media to investigate criminal activity.

We now share our data with the things in our lives as the next section will explain.

2.6 THE INTERNET OF THINGS

The term "Internet of Things" (IoTs) generally refers to things "such as devices or sensors – other than computers, smartphones or tablets – that connect, communicate or transmit information with or between each other through the Internet".[120] The IoTs is creating data within our homes; traditionally considered one of the most private of spaces. There are now more "things" connected to the internet than people.[121] Smart devices are becoming increasingly popular. It is expected that by 2020 there will be 50 billion internet connected devices.[122] The

[119] RCMP, "National Child Exploitation Coordination Centre" online: http://www.rcmp-grc.gc.ca/ncecc-cncee/about-ausujet-eng.htm.
[120] Federal Trade Commission, FTC Staff Report "Internet of Things: Privacy & Security in a Connected World" (January, 2015) online: www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf, page 6.
[121] *Ibid*, page 1. As of 2006 "the for the first time, the number of "things" connected to the Internet surpassed the number of people", quoting CISCO report.
[122] CISCO report, page 3.

IoTs has become common to many Canadian households in the form of wearable technology (such as smart watches, fitness trackers and medical devices), connected automation systems (adjusting light bulbs, coffee machines,[123] music and temperature), smart TVs[124], baby monitors[125], security systems, appliances, etc.[126] As one writer put it, "the physical and the digital world blur into each other".[127] The World Bank is even hoping to "harness big data from the Internet of Things (IoT) to help end extreme poverty and unlock new drivers of economic growth".[128]

Connected devices are used for energy efficiency, entertainment, wellness, home safety, home comfort, daily tasks and connectivity. IoTs gather large quantities of information about private activities, preferences and habits in the home to optimize the function of the device.[129] We regularly face encroachments on our privacy in exchange for perceived positive benefits we get from handing over our personal information.[130]

These connected devices claim to make life easier but will also record, collect, transmit, store, analyze and share vast amounts of personal information, such as exact location, financial account numbers, specific health information, details regarding personal habits, patterns of behaviour and preferences. This is mass data collection taken to the extreme. Smart devices can

[123] See *The Spy in the Coffee Machine*, page 8-9.
[124] Angela Hunt, "Your TV May Be Spying on You," Law Technology News (November 25, 2013).
[125] Wired, "Hackers are Exploiting Baby Monitors, But We Know How to Stop Them" (October 15, 2013) online: http://www.wired.com/gadgetlab/2013/10/baby-monitor-hacking/.
[126] See for example, Canadian Tire, "Nest" Products online: http://www.canadiantire.ca/en/nest.html, "Nest products are more than smart – they're thoughtful". See also, Fitbit, "Shop Versa" online: https://www.fitbit.com/en-ca/shop/versa "a heath & fitness smartwatch that lasts 4+ days and features 24/7 heart rate, phone-free music, apps, coaching & more". See generally, *The Spy in the Coffee Machine.*
[127] *The Spy in the Coffee Machine*, page 185.
[128] The World Bank, "World Bank Group and GSMA Announce Partnership to Leverage IoT Big Data for Development" (February 26, 2018) online: http://www.worldbank.org/en/news/press-release/2018/02/26/world-bank-group-and-gsma-announce-partnership-to-leverage-iot-big-data-for-development.
[129] Wired, "Internet of Things: Where does the Data Go?" online: https://www.wired.com/insights/2015/03/internet-things-data-go/.
[130] *The End of Privacy*, page 135.

easily be used as tools of invasive surveillance. These different devices have varying levels of data intrusion, from the mundane to the extremely personal.[131] Smart devices can be used to spy on their owners since they record and track their users' movements, actions and words in a most exact way. Fitbit has even been partially credited with solving a murder investigation.[132] It should not be surprising that companies have plans to put all these devices together to create "smart cities". There have been proposals for a "smart city" in Toronto, Ontario. Sidewalk Labs, an Alphabet subsidiary, proposal provides: "Welcome to Quayside, the world's first neighbourhood built from the internet up… with connectivity designed into its very foundation."[133] The imagined city will have cameras deployed to cover the entire space and systems will detect when trash bins need to be emptied.[134] Sensors will detect air quality, noise levels, flow of vehicles, cyclists, buses, pedestrians and weather.[135] It is expected that there would be thermal, electric and cost savings.[136] The idea is that the data will provide insight to run the city most efficiently. This new, "unimagined extreme" of data collection creates obvious privacy concerns.[137] This city of surveillance tracks every activity to learn residents' habits and adapt. Sidewalk Lab's chief policy officer, Rit

[131] Stefan Ducich, "These Walls *Can* Talk! Security Digital Privacy in the Smart Home under the Fourth Amendment" (2017) 16 Duke Law & Tech Rev 278, at 280. As an example, a woman discovered she was pregnant after she posted her Fitbit data on a message board, Reddit. See CBC, "Couple finds out Wife is Pregnant, Thanks to Fitbit (and Reddit)" (February 12, 2016) online: http://www.cbc.ca/radio/asithappens/as-it-happens-friday-edition-1.3445891/couple-finds-out-wife-is-pregnant-thanks-to-fitbit-and-reddit-1.3445900.

[132] CBC, "Murdered Woman's Fitbit Logged Steps after Husband said she Died" (April 25, 2017) online: http://www.cbc.ca/news/technology/fitbit-murder-1.4084506.

[133] Sidewalk Labs, "Submission" (October 17, 2017) online: https://sidewalktoronto.ca/wp-content/uploads/2017/10/Sidewalk-Labs-Vision-Sections-of-RFP-Submission.pdf [Sidewalk Labs]. See also CBC, "Google Sister Company makes 'Bold Bet' with new Tech-focused Neighbourhood 'Sidewalk Toronto'" (October 17, 2017) online: http://www.cbc.ca/news/ canada/toronto/waterfront-toronto-announcement-1.4358683.

[134] Sidewalk Labs, page 70. See also, page 92 for outline of managing solid waste through a smart disposal chain.

[135] *Ibid*, page 72.

[136] *Ibid*, Page 87-89.

[137] CBC, "Welcome to the Neighbourhood. Have You Read the Terms of Service?" (January 16, 2018) online: http://www.cbc.ca/news/technology/smart-cities-privacy-data-personal-information-sidewalk-1.4488145.

Aggarwala explained that "If people directly see value to having more information collected about them, they will be willing participants".[138]

One of the newer and popular IoTs is the digital assistant. Amazon's Alexa[139] and Google's Home[140] are two of the more well-known versions. Alexa is a device that allows you to "play music, control your smart home, get information, news, weather, and more using just your voice".[141] Amazon advertises Alexa Smart Home Devices that "let you voice-control thousands of different smart home devices such as lights, switches, TVs, thermostats and more from over 1,200 unique brands". Millions of these devices have been sold and excitedly brought into homes across the world, traditionally one of the most private of spaces.[142] The Alexa's Terms of Use Policy provides:

> Amazon processes and retains your Alexa Interactions, such as your voice inputs, music playlists, and your Alexa to-do and shopping lists, in the cloud to provide, personalize, and improve our services.[143]

Alexa Interactions are defined as:

> all information related to your use of Alexa and Alexa Enabled Products, including your voice and other inputs, responses provided to you through Alexa, information we receive in connection with Third Party Services and Auxiliary Products you use, and information and content you provide or receive through the Alexa App.

---

[138] *Ibid*.
[139] Amazon, "Echo" online: https://www.amazon.ca/echo. According to their website: "Echo connects to Alexa—a cloud-based voice service—to play music, make calls, set alarms and timers, ask questions, check your calendar, weather, traffic, and sports scores, manage to-do and shopping lists, control smart home devices, and more—instantly".
[140] Google, "Google Home" online: https://store.google.com/ca/product/google_home. According to their website: "Get answers, play songs, tackle your day, enjoy your entertainment and control your smart home with just your voice."
[141] Amazon, "Echo & Alexa Devices" online: https://www.amazon.com/Amazon-Echo-And-Alexa-Devices/b?ie=UTF8&node=9818047011.
[142] CNBC, "Amazon's Alexa had a Breakout Holiday – People even used Echoes to buy more Echoes" (December 26, 2017) online: https://www.cnbc.com/2017/12/26/how-many-amazon-alexa-echoes-were-sold-over-the-2017-holidays.html. See also Business Insider, "Amazon's Alexa won Christmas this Year" (December 26, 2017) online: http://www.businessinsider.com/amazon-alexa-top-ios-android-app-christmas-day-echo-sales-2017-12.
[143] Amazon, "Alexa Terms of Use" online: https://www.amazon.com/gp/help/customer/display.html?nodeId=201809740.

Essentially, Alexa collects and retains all this information. There is no information about how long Amazon stores that data. Google Home's website indicates they keep the data "until you choose to delete it".[144] It is a microphone in your home ready to listen and record everything you say to it or to those around you.[145] It can make calls for you, text for you and essentially become entrenched in your everyday life, supposedly to make life easier. The threats to privacy through data breaches, hacks, security failures or malfunctions are not hard to imagine. One recent example made headline news. A woman in Oregon discovered that her Alexa had surreptitiously recorded a conversation between her and her husband and then sent the audio recording to a random person on their contact list.[146] The possibilities for law enforcement to use a digital assistant are almost limitless. They could effectively use an Amazon Alexa or Google Home as an audio recording device (aka a room probe) without ever having to enter the residence and risk being caught in the act of placing such a device.

Even data from your smart fridge can tell a lot about you. Every time a person opens the door, the time and date are stored in a database.[147] That activity can be monitored to establish patterns of activity of the resident. For example, if the fridge door opens every day between 7:15am and 7:45am and then again between 4:30pm and 5:30pm, the recipient of that data would be able to make an educated guess that the resident works a 9am to 5pm job and is not home during the day. That is not to say a fridge's data can precisely determine a person's routine but it can be

[144] Google, "Data Security & Privacy on Google Home" online: https://support.google.com/googlehome/ answer/7072285?hl=en.
[145] See discussion of the microphone at Amazon, "Alexa and Alexa Device FAQs" online: https://www.amazon.com/gp/help/customer/display.html?nodeId= 201602230.
[146] See Quartz, "An Oregon Family's Encounter with Amazon Alexa Exposes the Privacy Problem of Smart Home Devices" (May 25, 2018) online: https://qz.com/1288743/amazon-alexa-echo-spying-on-users-raises-a-data-privacy-problem/. And See, CNBC, "Amazon Echo Secretly Recorded a Family's Conversation and Sent it to a Random Person on their Contact List" (May 24, 2018) online: https://www.cnbc.com/2018/05/24/amazon-echo-recorded-conversation-sent-to-random-person-report.html.
[147] *The Spy in the Coffee Machine*, page 14-15.

added to a composition of information. For a police investigation, that data could be used to verify surveillance observations or to help determine the best time to conduct a covert entry into the home to gather physical evidence. If police suspect drug trafficking is being operated out of an apartment they will want to gain entry to that apartment to look around when no one is home. They will perhaps take photographs and samples of any drugs in the residence to add to the body of evidence against the suspect.

This new reality of IoTs will likely be the next technological frontier for the SCC to consider with respect to section 8 analysis. The *ability* of police to obtain data from the IoTs is almost unlimited yet the *lawfulness* of such searches is uncertain.

2.7 TECHNOLOGICAL TOOLS FOR CRIME

Technology facilitates new crimes and changes how traditional crimes are committed. In understanding technology we should keep in mind that the internet can be used to carry out cyberattacks, trafficking of drugs, explosives, and weapons, human smuggling, child exploitation, terrorist financing and money laundering, as well as a variety of other serious crimes without regard for national boundaries.[148] These crimes may be perpetrated on the surface web; that is, web sites indexed by search engines.[149] In addition to the surface web, there is a layer of the internet called the deep web, and beyond there the dark web. The deep web is made up of internet content that is not indexed by search engines, such as intranet sites and other sites accessible via login criteria.[150] The dark web, like the deep web, is not indexed and is designed to operate and

[148] United Nations Office on Drugs and Crime, "Comprehensive Study on Cyber Crime: Chapter 2 The Global Picture" (February 2013) online: https://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/ CYBER CRIME_STUDY_210213.pdf, at 23-51.
[149] Hal Berghel, "Which is More Dangerous – the Dark Web or the Deep State?", Out of Band, Computer (July 2017), at 86 [Berghel].
[150] Berghel, at 86.

be accessed anonymously. To access the dark web anonymously, certain software is required. The Onion Router (TOR) is one such type of software.[151] TOR was originally developed by the US Naval Research Laboratory to allow secure communications and to protect the online identity of American spies.[152] TOR is now free to download and operates to hide a user's IP address and browsing history; it is described as "an effective censorship circumvention tool."[153] Having the benefit of anonymity provides essential secrecy for military and intelligence officers, political dissidents, journalists and whistleblowers. However, online anonymizing services allow criminals to use the technology opportunistically, making law enforcement efforts more difficult in combating crime on the dark web.[154] This "rising popularity of encryption" makes law enforcement efforts increasingly difficult.[155]

Criminals often use cryptocurrency online to ensure their anonymity. Cryptocurrency is virtual money that is untraceable because it uses digital encryption technology. It offers many benefits, such as increased payment efficiency, accessibility and low transaction costs. While it has legal uses, cryptocurrency has essentially become "the new hidden suitcase full of unmarked bills".[156] Arguably the most well-known cryptocurrency is Bitcoin.[157] Bitcoin allows the exchange of money on the dark web to be entirely anonymous. It has become an essential "accessory to cybercrime",[158] and so closely associated with the dark web that it has been referred to as "drug barter tokens".[159] TOR, together with Bitcoin, has made digital black markets on the

[151] Other examples include: I2P, Freenet, Riffle, Hidemyass.com. For more technical details on the most widely used onion router, see TOR, "TOR: Onion Service Protocol" online: www.torproject.org/docs/hidden-services.html.en.
[152] *Cybercrime with Ben Hammersky*: Season 1, Episode 1 (Netflix, television series: September 1, 2015).
[153] TOR, "TOR: Overview" online: https://www.torproject.org/about/overview.html.en.
[154] Berghel, at 87.
[155] Sophia Vogt, "The Digital Underworld: Combating Crime on the Dark Web in the Modern Era" (2017) 15:1 Santa Clara JIL 104, at 114 ["The Digital Underworld"].
[156] CBC, "Ransomware Attack Reveals Bitcoin as an Accessory to Cybercrime: Don Pittis" (May 16, 2017) online: http://www.cbc.ca/news/business/ransomware-bitcoin-threat-cyberattack-1.4115344. ["Ransomware Attack"]
[157] There is also Litecoin, Peercoin, Ripple, Zcash, Feathercoin, etc.; see *Banking on Bitcoin* (Netflix, documentary: August 14, 2017) [*Banking on Bitcoin*].
[158] Ransomware Attack.
[159] Gawker, "The Underground Website where you can Buy Any Drug Imaginable" (June 1, 2011) online: http://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160 ["Underground Website"].

dark web possible.[160] One of the most successful drug markets on the dark web was the Silk Road.[161] A large percentage of sellers on the Silk Road are from Canada. [162] The Silk Road and other websites like it allow buying and selling of drugs on the dark web as easily as buying a book from Amazon or eBay.[163] Drug transactions are conducted openly on the site because the users enjoy anonymity. There is a "buffet for narcotics" readily available.[164] The creator of the Silk Road, Ross Ulbricht, boasted to Forbes magazine that "we've won the state's war on drugs because of Bitcoin".[165] Interestingly, the IoTs, crime and bitcoin come together. As a recent CBC news story explained, criminal hackers used smart appliances to mine bitcoins in a case known as a cryptojacking.[166] Martin Hron, a security researcher at antivirus developer Avast, warned that "the risk is growing as more everyday devices connect to the internet – from ovens to home lighting systems – and that these are often the least secure".[167]

There are few barriers to entry to the dark web: it requires little expertise, is quick and accessible. It is extremely difficult for law enforcement to determine a location or name of someone engaging in criminal behavior. To further complicate the matter, it operates transnationally through servers all over the world. The fact that a middle-class American college

---

[160] *Banking on Bitcoin*.
[161] Silk Road reported to have several million dollars a day in trade, *Inside the Dark Web*; reported 60,000 visits a day from Forbes, "Meet the Dread Pirate Roberts, the Man Behind Booming Black Market Drug Website Silk Road", (August 14, 2013) online: https://www.forbes.com/sites/andygreenberg/2013/08/14/meet-the-dread-pirate-roberts-the-man-behind-booming-black-market-drug-website-silk-road/ ["Meet DPR"]. The United States Attorney's Office, Southern District of New York, "Manhattan U.S. Attorney Announces The Indictment of Ross Ulbricht, the Creator and Owner of the "Silk Road" Website" (February 4, 2014) online: https://www.justice.gov/ usao-sdny/pr/manhattan-us-attorney-announces-indictment-ross-ulbricht-creator-and-owner-silk-road. Silk road was "used by several thousand drug dealers… to distribute hundreds of kilograms of illegal drugs… to well over a hundred thousand buyers, and to launder hundreds of millions of dollars"; Berghel, at 88 reported that the Silk Road "accounted for approximately $1.2 billion in sales to 960,000 customers from 2011 to 2013".
[162] "Underground Website"; See also CBC, "Canadians Among Top Participants on Illegal Drug Website" (August 16, 2012) online: http://www.cbc.ca/news/canada/canadians-among-top-participants-on-illegal-drug-website-1.1158116.
[163] "Underground Website".
[164] *Inside the Dark Web*.
[165] "Meet DPR"; Forbes, "An Interview with a Digital Drug Lord: The Silk Road's Dread Pirate Roberts (Q&A)" (August 14, 2013) online: https://www.forbes.com/sites/andygreenberg/2013/08/14/an-interview-with-a-digital-drug-lord-the-silk-roads-dread-pirate-roberts-qa/#32088c3a5732.
[166] CBC, "Your Smart Fridge could be Mining Bitcoins for Criminals" (June 29, 2018) online: https://www.cbc.ca/news/technology/bitcoin-hacking-smart-devices-1.4728222.
[167] *Ibid*.

student with a complete lack of criminal history and a "reputation for peacefulness" could become one of the biggest drug lords on the dark web demonstrates the powerful protection anonymity provides.[168] A reality has been created where a drug dealer who uses a computer is far less likely to face detection and prosecution than if they sold drugs on a street corner. This is because people can be identified and followed from a street corner, but they cannot be tracked or followed from the dark web because their IP address is hidden from view. The transactions are done in an open forum market; police can see the transactions but cannot identify the parties involved.[169]

In addition to the internet, communication technology assists criminals in evading law enforcement. While not created specifically for criminal use, these technologies certainly seem to be designed to maximize criminal activity. Encrypted communications are widely available.[170] Messages that auto-delete and video conversations that cannot be captured are the norm. It is impractical for law enforcement to decrypt or capture these types of communications. Remote Administration Tools (RATs) are another technological advancement that criminals employ. RATs allow a user to control their devices remotely. It does not take much imagination to guess how a criminal could benefit from such technology. Remote erasing of messages is useful if a criminal's phone is seized by police. The ability to take a photograph and pinpoint a GPS location when a phone is accessed is useful if a police agent or the police are covertly accessing the device. The criminal then knows the device was accessed by someone other than themselves and can capture a photograph of that person. If the person accessing the device is a confidential informant or police agent, the criminal has captured their images. These counter surveillance methods allow criminals to detect and avoid police presence. The safety of police confidential informants and undercover officers can be at serious risk if a criminal has a RAT on their device. Police must

[168] Joshua Dratel, Letter (November 19, 2013) online: http://www.libertyunderattack.com/wp-content/uploads/2015/06/131119-Letter-Submitted-in-Support-of-Application-for-Ross-Bail.pdf.
[169] "The Digital Underworld", at 118.
[170] Examples include: PGP, Skype, Telegram, WhatsApp, Hushmail, Cryptocat.

prepare and tailor their investigations for a level of sophistication made possible by the proliferation of these types of technologies, which are cheap and easy to obtain.

These technologies allow individuals to hide behind enhanced privacy to commit crimes online or organize criminal activities through encrypted online communications. Some of the technological abilities are seemingly crafted specifically for the criminal underworld. As the Canadian Association of Police Chiefs explained:

> Digital security technology has now advanced to the point that impenetrable password protection and encryption are readily – and in many cases freely – available on all electronic devices. This technology immunizes legally seized electronic devices from the execution of a judicially authorized search, and often compels the abrupt and unsuccessful end of a serious criminal investigation. Recent law enforcement experience provides specific examples of criminal investigations that have been derailed in this manner.[171]

The reality is that these technologies provide a level of sophistication to criminals that was previously reserved for serious organized crime groups with technical skills. As a result, law enforcement has limited success in investigating and capturing criminals who take advantage of technology and anonymity.[172]

The right of an individual to use the internet anonymously and employ tools to evade law enforcement must be weighed against society's need to counter the threat to public order and security that takes place on the internet. In spite of its many social benefits, the internet is a powerful tool in the hands of those who use it to do harm.

---

[171] Canadian Association of Chiefs of Police, "Resolutions adopted at the 111th Annual Conference" (Ottawa, Ontario: August 2016) online: https://www.cacp.ca/resolution.html?asst_id=1197, at 21.

[172] For example, the Westminster Bridge attacker used the online service WhatsApp to send an encrypted message just minutes before the rampage that left three civilians and one police officer dead. Because WhatsApp provides encryption to photos, videos and voice calls, they are providing terrorists a secret place to communicate with each other. See CBC, "Khalid Masood reportedly used WhatsApp minutes before London Attack" (March 26, 2017) online: http://www.cbc.ca/news/world/social-media-terrorism-whatsapp-encryption-1.4041574. See also, WhatsApp website which brags about their services encryption capabilities: WhatsApp, "WhatsApp" online: https://www.whatsapp.com/.

2.8 CONCLUSION

The foregoing review of some highlights of our technological reality – mass data collection, prevalence of data breaches, surveillance as entertainment, social media and the IoTs – shows how technology now forms part of many criminal investigations. Technology acts as a scrupulous record keeper automatically compiling data of our activities. Most people are unaware and ignorant of the fact that most of their devices and applications compromise their privacy.[173] All this data can be tremendously beneficial to criminal investigations and prosecutions. The next chapter will look at how section 8 of the *Charter* aims to protect that data against unreasonable searches and seizures.

[173] *The Spy in the Coffee Machine*, page 217.

CHAPTER 3: UNREASONABLE SEARCH AND SEIZURE UNDER SECTION 8 OF THE *CHARTER*

3.1 INTRODUCTION

This project explores the distinct sphere of informational privacy within section 8 case law and specifically how the law concerning informational privacy should adapt to emerging technologies. With the development of the Internet of Things (IoTs), the Supreme Court of Canada (SCC) will likely soon be forced to consider the boundaries of informational privacy in this new technology. This chapter outlines the development and current state of the law on section 8 of the *Charter* which is necessary to understand the analysis in chapters 4, 5 and 6. The SCC has interpreted section 8 of the *Charter* as requiring a normative inquiry, focusing on the concept of a reasonable expectation of privacy. The normative quality of the section 8 inquiry is explained in section 3.2. Section 3.3 then explains how the SCC strives to achieve a balance between law enforcement efforts and individual privacy interests. Section 3.4 introduces two of the main tools of analysis employed by the Court in section 8 cases. This chapter aims to inform the reader of foundational section 8 principles before moving on to explore the challenges specific to their application to technology.

The SCC has consistently identified three distinct spheres of privacy deserving of constitutional protection – spatial, personal and informational.[174] These privacy interests are distinct from one another but commonly overlap.[175] Spatial privacy, also termed territorial

[174] *R v Dyment*, [1988] 2 SCR 417, 66 CR (3d) 348 [*Dyment*], para 45. See also, *Tessling*, para 20; *R v Patrick*, 2009 SCC 17, [2009] 1 SCR 579 [*Patrick*], para 42; *Gomboc*, para 19.

[175] *Gomboc*, para 19. Informational privacy will commonly involve territorial privacy interests in a person's home or physical area where they maintain computers or cellphones. In *Gomboc*, Justice Deschamps explained that when a case is essentially an informational privacy one, a territorial privacy aspect "should not be allowed to inflate the actual impact of the search to a point where it bears disproportionately on the expectation of privacy analysis" para 50. In *Patrick*, the SCC dealt with informational privacy in relation to a "bag of information", but territorial aspects were significant to the analysis, see Richard Jochelson, "Trashcans and Constitutional Custodians: The Liminal Spaces of Privacy in the Wake of Patrick" (2009) 72 Sask L Rev 199 ["Trashcans and Constitutional Custodians"], page 11.

privacy, involves one's privacy in places. For example, one has territorial privacy in one's home or vehicle. Personal privacy relates to bodily integrity; to one's body and bodily substances. Informational privacy has been defined 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".[176] The SCC initially addressed informational privacy in *R v Dyment*.[177] In that case, a doctor collected a blood sample from an unconscious patient and provided it to police for their investigation into a motor vehicle accident. Personal privacy and the confidentiality of a doctor-patient relationship weighed heavily in the SCC majorities' decision to exclude the evidence from trial.[178] In the reasons for judgement, Justice LaForest adopted a view of informational privacy from the Department of Justice Task Force on Privacy and Computers. He cited the Task Force report, saying: "This notion of [informational] privacy derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit".[179] Essentially, informational privacy is concerned with that information about our lives that should be protected from disclosure to the State.

3.2 A NORMATIVE AND NEUTRAL INQUIRY

The *Canadian Charter of Rights and Freedoms* forms part of the *Constitution of Canada, 1982*; being "the supreme law of Canada".[180] Since the *Charter* forms part of the *Constitution* it

[176] *Tessling*, para 23, citing A.F. Westin, *Privacy and Freedom* (1970) page 7. This definition of information privacy has also been used by the SCC in *Gomboc*, para 19; *Cole*, para 42; *R v Spencer*, 2014 SCC 43, [2014] SCR 212 [*Spencer* SCC], para 40 and *Marakah*, para 39.
[177] *Dyment*.
[178] In *Dyment*, the SCC recognized that the seizure of blood samples from the wound of an accident victim infringed on all three spheres of privacy.
[179] *Dyment*, para 33, citing Task Force on Privacy and Computers, Privacy and Computers (1972), page 12-14, 23.
[180] *Charter,* section 52(1). The "Constitution of Canada" is defined in section 52(2) of the *Constitution Act, 1982*, and the definition includes "this Act" of which the *Charter* is Part I.

requires a flexible interpretation that can adapt to changes over time, including changing societal values.[181] The SCC, in *Hunter v Southam* specifically adopted this flexible interpretation for section 8 of the *Charter*.[182] Justice Dickson (as he then was), in writing the unanimous judgment, explained that section 8 "must be capable of growth and development over time to meet new social, political and historical realities often unimagined by its framers".[183] To achieve this flexibility, section 8 of the *Charter* should be given a "broad, purposive analysis".[184] The SCC identified the purpose of section 8 as to *prevent* unjustified state intrusion on individual privacy.[185] *Hunter v Southam* continues to be a seminal judgement for section 8 cases as it recognized an "individual's right to privacy".[186] Individuals charged with a criminal offence regularly challenge searches that have led to the seizure of incriminating evidence in the hopes that the evidence will be excluded from their trial under section 24(2) of the *Charter* and they will avoid a guilty verdict. They argue a violation of their section 8 *Charter* right to be free from unreasonable search and seizure.

Section 8 protects against *unreasonable* search or seizure and, therefore, only protects a *reasonable* expectation of privacy.[187] In *R v Cole*, Justice Fish plainly stated "[p]rivacy is a matter of reasonable expectations".[188] A diminished expectation of privacy is still reasonable and attracts section 8 *Charter* protection; subject to intrusion only with lawful authority.[189] Where there is an

---

[181] See *Hunter v. Southam*, para 16. See also Peter Hogg, *Constitutional Law of Canada*, Student Edition (Toronto: Carswell, 2015), pages 36-25 to 36-26 [Hogg]. See also *Hunter v Southam*, para 16.
[182] *Hunter v Southam*.
[183] *Hunter v Southam*, para 16.
[184] *Hunter v Southam*, paras 18-19 and 26; see also Stuart, page 290.
[185] *Hunter v Southam*, paras 25 and 27.
[186] *Hunter v Southam*, para 32. James Fontana and David Keeshan, eds. *The Law of Search and Seizure in Canada*, 9th ed (Toronto: LexisNexis Canada Inc., 2015) [Fontana], page 4.
[187] *Hunter v Southam*, para 25; *Gomboc*, para 20.
[188] *Cole*, para 35.
[189] *Tessling*, para 42; *Cole*, paras 3 and 9. In *Cole*, the fact that the computer was a work laptop lowered the accused's expectation of privacy in the device, but the SCC recognized he maintained a reasonable expectation of privacy. Note, certain situations – state border crossing, school, prison – are commonly known to attract a lesser expectation of privacy. For example, at a border crossing, people expect they may be questioned or searched by customs officers as permitted by the *Customs Act*, RSC 1985, c 1 [*Customs Act*]. See also Fontana, pages 21-24.

intrusion on any reasonable expectation of privacy, the state action will be considered a "search" for section 8 purposes.[190] Two distinct questions arise in every section 8 analysis. The first question asks: Does the accused have a reasonable expectation of privacy, such that a search or seizure has taken place?[191] If the answer to this question is no, there is no section 8 *Charter* issue. If the answer to the first question is yes, the analysis must continue to the second question: Was the search or seizure an unreasonable intrusion on that privacy?[192] *Hunter v Southam* established prior authorization as a "precondition for a valid search and seizure".[193] There are some situations which allow for warrantless searches, such as searches incident to lawful arrest, but the SCC set out the default standard to achieve. Any search involving a *Charter* protected privacy interest will be considered reasonable if it is authorized by law, the law itself is reasonable, and the search is conducted in a reasonable manner.[194] A search conducted under the authority of a warrant is presumptively reasonable, having satisfied a judicial authority that there are sufficient reasonable and probable grounds for the search.[195] Alternatively, a warrantless search attracts a presumption of unreasonableness.[196] This system of prior authorization, instead of after-the-fact validation, avoids a justification mentality. It is important to note that the consequence of this framework means that if there is no reasonable expectation of privacy, there is no requirement to obtain prior authorization. Therefore, whether there is any reasonable expectation of privacy is effectively a threshold question.

---

[190] *Hunter v Southam*, para 25. See also Stuart, page 295.
[191] Fontana, page 4.
[192] *R v Edwards*, [1996] 1 SCR 128, 123 DLR (4th) 31, para 33 [*Edwards*]; *Jones*, para 11.
[193] *Hunter v Southam*, para 29, see also paras 27 and 28.
[194] *R v Collins*, [1987] 1 SCR 265, 33 CCC (3d) 1 [*Collins*], para 34.
[195] *Criminal Code*, s 487; *Gomboc,* para 20.
[196] *Hunter v Southam*, para 30. See also Fontana at page 5.

Framing section 8 cases using a normative inquiry is required in order to achieve the *Charter*'s purposive approach. In *Tessling*, the SCC explained that the inquiry into whether a person has an expectation of privacy "is a normative rather than descriptive standard".[197] The Court asks what information *ought to be* protected by section 8, not whether it actually is protected.[198] For example, in *Dyment*, the patient did not *actually* maintain control or privacy over the blood sample when it was taken by the doctor and given to the police, but he nevertheless maintained a reasonable expectation of privacy in it. The Court recognized that taking a blood sample from an unconscious person without their consent by a doctor is a violation of one's dignity and privacy that should not be accepted in our society.[199] In *R v Plant*, Justice Sopinka, writing for the majority, dealt with an informational privacy case. In finding that there was no reasonable expectation of privacy in computerized electricity records maintained by the utility,[200] he explained:

> In fostering the underlying values of dignity, integrity and autonomy, it is fitting that s. 8 of the *Charter* should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state.[201] [emphasis added]

We can wish to retain control over our information and keep it from the State, even if that is not the reality of the situation. Plant did not have actual control over his electricity records held by the utility company but would wish to maintain control from State access. The fact that an Internet Service Provider (ISP) or technology company *can* provide information to the police does not make it reasonable nor lead to the conclusion that a reasonable expectation of privacy has

[197] *Tessling*, para 42. "Normative" is defined as "relating to, or determining norms or standards", Merriam-Webster "Normative" online: https://www.merriam-webster.com/dictionary/normative. Note, the term is not judicially defined.
[198] See *Spencer* SCC, para 18.
[199] *Dyment*, para 39 and 45.
[200] *Plant*, para 30.
[201] *Plant*, para 27.

disappeared on a normative analysis.[202] The SCC uses this normative approach to secure our privacy interests. In fact, the SCC has explicitly rejected a "risk analysis" approach to section 8 cases which focuses on the risk that those guilty of wrongdoing have assumed.[203] According to the Court:

> … privacy would be inadequately protected if an assessment of the reasonableness of a given expectation of privacy were made to rest on a consideration whether the person concerned had courted the risk of electronic surveillance. In view of the advanced state of surveillance technology, this would be to adopt a meaningless standard for, in the final analysis, the technical resources which agents of the state have at their disposal ensure that we now run the risk of having our words recorded virtually every time we speak to another human being.[204]

If the Court were to adopt the risk analysis instead of rejecting it, they would have to consider the technological realities of today. As early as 1990, the SCC recognized that "modern methods of electronic surveillance have the potential, if uncontrolled, to annihilate privacy".[205] Since then, online privacy has really become something of an oxymoron. In August 1997, Time Magazine's cover story entitled "The Death of Privacy" stated: "You have no secrets. At the ATM, on the Internet, even walking down the street, people are watching your every move."[206] As one popular 2017 drama series character explained: "we gave that [privacy] up a long time ago so we could watch cat videos on our phones."[207] The impressive growth in technology has fundamentally altered our expectations about what will be private; it has "shifted our thinking about what should be private".[208]

---

[202] See *Spencer* SCC.
[203] See for example *R v Sanelli*, [1990] 1 SCR 30, 53 CCC (3d) 1 [*Duarte*]; *R v Wong*, [1990] 3 SCR 36, 1 CR (4th) 1 [*Wong*] and *Cole*.
[204] *Wong*, para 11.
[205] *Wong*, para 15.
[206] Time Magazine, "Death of Privacy" (August 25, 1997) online: http://content.time.com/time/covers/0,16641,19970825,00.html.
[207] *Wisdom of the Crowd*: Season 1, Episode 1 (Global TV, television series: October 1, 2017).
[208] *Blown to Bits*, page 21.

The SCC has made reference to George Orwell's novel *1984*, based on a dystopian surveillanced world, numerous times over the years.[209] In *Tessling*, Justice Binnie for a unanimous Court quoted 1984 to make the point that "technological surveillance raises extremely serious concerns".[210] Justice Binnie again in *M(A)* referred to *1984*, stating: "the fact is that 1984 came and went without George Orwell's fears being entirely realized, although he saw earlier than most the direction in which things might be heading."[211] In *Fearon*, Justice Karakatsanis in dissent made the statement that "as technology changes, our law must also evolve so that modern mobile devices do not become the telescreens of George Orwell's *1984*".[212] Nonetheless, some argue that "1984 is here, and we like it".[213] Orwell imagined cameras everywhere – that is our reality. And cameras are not the most pervasive of today's tracking technologies. Some have equated our hyper-surveillance society with a panopticon.[214] Numerous authors have asserted that we now live in a "post-privacy world"[215] where we have swapped privacy for a plethora of perks only dreamt of a decade ago.[216] As one author put it: "Modest incentives induced individuals to sacrifice their personal privacy – often before they understood what they were giving up…The next generation may not even see the loss of privacy as a sacrifice."[217] With the pervasiveness of technology in

[209] See *Wise*, para 76; *Wong*, para 15; *Tessling*, *Fearon*, para 102; and *M(A),* 2008 SCC 19, [2008] 1 SCR 569 [*M(A)*].
[210] *Tessling*, para 54.
[211] *M(A)*, para 40.
[212] *Fearon*, para 102.
[213] *Blown to Bits*, page 19; and see page 20: "We have fallen in love with this always-on world."
[214] *The Spy in the Coffee Machine*, page 211: "Our digital technologies have created panopticon"; and see *End of Privacy*, page 33: reference to power of surveillance in contemporary world creating panopticon effect.
[215] See for example: *The Spy in the Coffee Machine*, page 182 "Privacy as many of us grew up knowing it is gone forever, thanks to technology (think of pinhole video cameras and the spyware that turns on the camera and microphone on a cell phone)." and "The privacy which a person could have expected in the 1990s has gone forever" page 232; *The End of Privacy*; *Social Networks and the Death of Privacy*; *Big Data*, page 163, "big data erodes privacy"; Deckle McLean, *Privacy and Its Invasion* (London: Praeger publishers, 1995), on page ix: "privacy is in crisis"; see also "If You Don't Care about Privacy".
[216] See *Blown to Bits*, page 20; *The Spy in the Coffee Machine*, page 10, 212; Renee Pomerance, "Flirting with Frankenstein: The Battle between Privacy and Our Technological Monsters" (2016) 20 Can Crim LR 149 ["Flirting with Frankenstein"], 154-155.
[217] *Blown to Bits*, page 296.

society, "we have become unwitting, or perhaps, all too willing, participants in our own privacy invasions."[218] The Court has been using the normative approach to assessing section 8 privacy interests in such a way so as to protect us from this reality. By asking what privacy we ought to have, instead of that which is actually available to us, section 8 protects a larger sphere of our information.

The SCC has continually held that it is important to frame the question as a *neutral* query.[219] This means that the nature of the privacy interest does not depend on whether the privacy protects legal or illegal activity.[220] A court's analysis must ignore the results of the search to avoid any after-the-fact justification and maintain section 8's purpose to prevent unjustified searches. In *R v Wong*, the accused was found operating an illegal gambling operation in a hotel room. Framing the question in broad and neutral terms meant asking whether "persons who retire to a hotel room and close the door behind them have a reasonable expectation of privacy?"[221] In *R v Patrick*, the police searched the household trash of the accused left out for collection and found evidence of an ecstasy lab.[222] The SCC explained:

> The issue is not whether the appellant had a legitimate privacy interest in the concealment of drug paraphernalia, but whether people generally have a privacy interest in the concealed contents of an opaque and sealed "bag of information".[223]

This neutral framing of the search question continues to be the preferred approach to section 8 cases.[224]

---

[218] "Flirting with Frankenstein", at 154.
[219] *Wong*, para 20. See also, Stuart, page 295.
[220] *Spencer* SCC, para 36. Fontana, page 17.
[221] *Wong*, para 20.
[222] *Patrick*, para 3. See "Trashcans and Constitutional Custodians" for full discussion of the *Patrick* judgment.
[223] *Patrick*, para 32.
[224] See for example, *Spencer* SCC and *Marakah* wherein the SCC framed the question in neutral terms, internet activity and electronic text message conversation, without reference to the illegal nature of the activity.

Almost all of the litigation involving section 8 of the *Charter* deal with individuals who we know are factually guilty of the charges alleged. The temptation to assume that the charged person is always guilty must be resisted however as innocent persons are subject to the same police conduct.[225] In addition, most criminal cases are actually disposed of without a trial, so no judgment is ever written on the search. Because of these considerations, we must be open minded and consider the constitutional protections as though all individuals are factually innocent.

3.3 BALANCING VALUES

It is important to understand that once it has been established that there is a reasonable expectation of privacy (the threshold question), the task of any section 8 analysis is to balance competing values; individual interests and rights against our collective preference and desire for security. Section 8 of the *Charter* "is concerned with the degree of privacy needed to maintain a free and open society".[226] The SCC articulated the balancing in *Hunter v Southam* as follows:

> … an assessment must be made as to whether in a particular situation the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals, notably those of law enforcement.[227]

The SCC has explained that the balance is a "delicate"[228] one between privacy and law enforcement interests that must be "calibrated according to the circumstances".[229] The competing

[225] See for example *R v Calderon* [2004], 23 CR (6th) 1, 188 CCC (3d) 481, paras 71-72. Police were relying on "indicators" of drug trafficking to stop motor vehicles, yet they were neutral and could be found in any vehicle. In fact, one officer relied on the "indicators" to stop between 50 to 100 vehicles with no resulting arrests. Many times, investigative techniques are employed and while they search multiple individuals, only one case results in charges and is litigated. See also *Spencer*, wherein the practice of police making requests to Internet Service Providers (ISPs) for consumer information without a production order was common.
[226] *R v Ward*, 2012 ONCA 660, [2012] 112 OR (3d) 321 [*Ward*], para 86.
[227] *Hunter v Southam*, para 25.
[228] *Marakah*, paras 100 and 114.
[229] *R v Kang-Brown*, 2008 SCC 18, [2008] 1 SCR 456 [*Kang-Brown*], para 24.

values involved are interrelated[230] and the weight placed on these values changes over time.[231] The system of prior authorization allows a judicial actor to balance the conflicting interests of the state and individual; only where the state's interests are demonstrably superior and compelling will the search be authorized.

Privacy is meant to protect "individuality, autonomy, dignity, emotional release, self-evaluation, and interpersonal relationships".[232] While privacy "is at the heart of liberty in a modern state",[233] it must be subject to limits. When speaking with students from the University of Toronto's Faculty of Law, in an interview for their student newspaper *Ultra Vires* at the end of 2014, Justice Abella explained: privacy law must allow "enough space for individual dignity and autonomy" but must also "acknowledge public interests that may be countervailing".[234] Suppression of crime is a legitimate societal value. The state has an obligation to citizens to uphold the law and protect them against criminal activity. As concisely put by Justice Binnie in *R v Tessling*, the "community wants privacy, but it also insists on protection".[235] And Justice Arbour noted in *B(SA)*, "[e]ffective law enforcement benefits society as a whole".[236] There must be a balanced approach to the reasonable expectation of privacy. Desires are high on both sides of the equation – people would like total privacy protection from the State and police would like open

[230] Arthur Cockfield, "Protecting the Social Value of Privacy in the Context of State Investigations using New Technologies" (2007) 40 UBC L Rev 41.
[231] See *Spencer* SCC, para 15; *Fearon*, paras 112-125.
[232] "The Digital Underworld", at 107.
[233] *Dyment*, at paras 17 and 28.
[234] Tali Green and Grett Hughes, "Justice Abella on Privacy, Decision-Writing, and the Role of Law Schools" (2014) Ultra Vires October 29, at 6. Also available online: http://ultravires.ca/2014/10/ justice-abella-on-privacy-decision-writing-and-improving-law-schools/.
[235] *Tessling*, para 17.
[236] *R v B(SA)*, 2003 SCC 60, [2003] 2 SCR 678, para 51.

access to all our information with no barriers to access. It is a "matter of degree rather than an all-or-nothing distinction".[237]

The SCC consistently views privacy as an individual right, essential for personal autonomy and dignity, and a societal good necessary for democracy.[238] They hold that it allows individuals the freedom to debate, associate and organize free from state surveillance. This view of section 8 protection as an individual claim and privilege is not inherent to section 8 but it does affect how the discussion unfolds. In *Edwards*, the SCC was asked whether a boyfriend had any section 8 privacy protection in evidence obtained from his girlfriend's apartment. A majority of the Court framed the privacy question as a personal right issue.[239] Justice Cory explained:

> Since no personal right of the appellant was affected by the police conduct at the apartment, the appellant could not contest the admissibility of the evidence pursuant to s. 24(2) of the *Charter*. It is therefore not necessary to consider either this aspect of the case or whether Ms. Evers did in fact consent to the search of her apartment. This is, in itself, a sufficient basis for dismissing the appeal.[240]

Justice LaForest expressly disagreed with the majorities characterization of the right to be free from unreasonable search and seizure. In his dissenting judgement he wrote:

> … I am deeply concerned with the implications of these reasons which, I think, result in a drastic diminution of the protection to the public that s. 8 of the *Canadian Charter of Rights and Freedoms* was intended to ensure.
>
> …
>
> As I see it, the protection accorded by s. 8 is not in its terms limited to searches of premises over which an accused has a personal right to privacy in the sense of some direct control or property. Rather the provision is intended to afford protection to all of us to be secure against intrusion by the state or its agents by unreasonable searches or seizures …. The section, it must be remembered, reads: "*Everyone* has the right *to be secure* against unreasonable search or seizure" (emphasis added). It

[237] "Privacy and the Reasonable Paranoid", at 321.
[238] *Hunter v Southam*.
[239] *Edwards*, para 45.
[240] *Edwards*, para 51.

> is a right enuring to all the public. It applies to *everyone*, an expression that unlike many of the other *Charter* provisions is not qualified by express circumstances, such as, for example, s. 9 which protects everyone arbitrarily detained or imprisoned, s. 10, which applies to everyone arrested or detained, and s. 11, which is limited to a person charged with an offence. Moreover, s. 8 does not merely prohibit unreasonable searches or seizures, but also guarantees to everyone the right to be *secure* against such unjustified state action… It is a public right, enjoyed by all of us.
>
> …
>
> The issue has not yet been directly raised because the cases dealt with in this Court have thus far been centered on cases of unreasonable searches directly involving the personal expectation of privacy of an accused person. But the approach I am suggesting is entirely consistent with the conceptual, societal and constitutional underpinnings of the right guaranteed by s. 8….

As Justice LaForest noted back in 1996, section 8 did not have to be limited as an individual right but rather could be viewed as a collective value, recognizing with our shared values of sociality, connectiveness and openness. Yet the Court consciously has framed privacy as an individual right. The implications of framing section 8 protection as an individual, instead of a collective, right is explored further in chapter 5 where I discuss options for moving forward with a clearer section 8 jurisprudence. For now, it is significant to note that the balancing of rights is restricted by the individual considerations on one side against with societal protection on the other.

3.4 TOOLS OF ANALYSIS FOR SECTION 8 ANALYSIS

This section introduces the reader to two main tools of analysis employed by the Court in section 8 cases. An understanding of these tools is necessary to appreciate what challenges they present and what changes are required to improve section 8 jurisprudence moving forward.

3.4.1 The Biographical Core

The SCC has often expressed the view that section 8 of the *Charter* should seek to protect a biographical core of personal information, including information which tends to reveal intimate details of lifestyle and personal choices. The concept has experienced broad acceptance in its application but has seemingly waned over time.

A biographical core of information was first discussed by the SCC in 1993 in the *Plant* case. This was the first time the SCC considered the search of computer records[241] and there was uncertainty as to how to treat them. Police had obtained a search warrant for a residence based on a tip, observations from a perimeter search and results of a comparison of computerized electricity records. The search found 112 marihuana plants. The trial judge had found that the records check was not a search for section 8 purposes because the records did not belong to the accused. The Court of Appeal agreed, holding that the information belonged to the Calgary Utilities Commission and had been created in the context of a commercial relationship. They found that the computer search did not violate section 8. One of the questions for consideration on appeal to the SCC was whether the police check of the computerized electrical records violated section 8. Justice Sopinka, for the majority at the SCC, articulated a framework for determining the nature and extent of a reasonable expectation of privacy of information. In finding that the homeowner had no reasonable expectation of privacy in electricity records maintained by the utility, he explained:

> In order for constitutional protection to be extended to commercial documents, the information seized must be of a personal and confidential nature. In fostering the underlying values of dignity, integrity and autonomy, it is fitting that s. 8 of the Charter should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to

[241] *Plant*, para 24.

> reveal intimate details of the lifestyle and personal choices of the individual.[242] [emphasis added]

This first framing of the biographical core attempts to delineate what information is protected by section 8; the idea being that not *all* information attracts equal constitutional protection. If information is part of one's biographical core, it will undoubtedly attract privacy protection without further inquiry.[243] Plant had failed to bring the computer search within the parameters of section 8. It is interesting to note that Chief Justice McLachlin, in separate reasons, concurring in the result, would have included the very fact of criminality as part of the lifestyle of the accused. In finding he did have a reasonable expectation of privacy in the records, she wrote: "the very reason the police wanted these records was to learn about the appellant's lifestyle, i.e. the fact that he was growing marihuana".[244]

In *Tessling*, the biographical core of information was central in the SCC's assessment. In that case, police used a forward looking infrared (FLIR) device to take a heat image of the accused's home from an aircraft. Based on the information from that image and information from informants, police were able to obtain a search warrant for the residence where they found a large quantity of marihuana and several guns. Justice Binnie, writing for a unanimous Court, cited *Plant* and explained that "not all information an individual may wish to keep confidential necessarily enjoys s. 8 protection".[245] The judgment goes on to ask: "Did the FLIR heat profile expose any intimate details of the respondent's lifestyle or part of his core biological data?"[246] The conclusion was that:

---

[242] *Plant*, para 27.
[243] Note, if the information in question does not form part of one's biographical core, that does not end the analysis but rather a court would consider other indicia to determine if the information is privacy protected.
[244] *Plant*, para 49.
[245] *Tessling*, para 26.
[246] *Tessling*, para 59.

> The information generated by FLIR imaging about the respondent does not touch on "a biographical core of personal information", nor does it "ten[d] to reveal intimate details of [his] lifestyle.[247]

There was ultimately no reasonable expectation of privacy in the information and therefore no search for section 8 purposes.

Plant and *Tessling* demonstrate the use of the biographical core as a tool of analysis. In both cases, the information (electricity consumption and heat profile) did not form part of the biographical core or reveal intimate details of lifestyle. The fact that the information in question was not part of the biographical core weighed heavily in favor of finding that there was no reasonable expectation of privacy and therefore no constitutional protection. The significance of the biographical core was at its height in these two cases. When used, the biographical core seems to limit the scope of section 8 by restricting the type of information deserving of protection to that which is intimate, personal and commonly considered private. To put it another way, when information reveals a person's biographical core, rather than mundane information, it attracts the strongest privacy protections.[248]

The 2012 judgment of *Cole* is another example of the SCC using the biographical core a part of the section 8 analysis. In *Cole*, a computer technician found child pornography on a teacher's work assigned laptop. The school gave the laptop to the police without a search warrant. The question for the Court was whether there was a reasonable expectation of privacy in the laptop's contents such that police should have obtained a search warrant before they conducted their examination. Both Justice Fish for the majority and Justice Abella in dissent found a breach of section 8. The majority judgment begins with a statement that computers "contain information

[247] *Tessling*, para 62.
[248] See "Trashcans and Constitutional Custodians", at 204.

that is meaningful, intimate, and touching on the user's biographical core".[249] This is developed later in the judgment when Justice Fish explained:

> 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.
>
> Computers that are used for personal purposes, regardless of where they are found or to whom they belong, "contain the details of our financial, medical, and personal situations" (*Morelli*, at para. 105). This is particularly the case where, as here, the computer is used to browse the Web. Internet-connected devices "reveal our specific interests, likes, and propensities, recording in the browsing history and cache files the information we seek out and read, watch, or listen to on the Internet" (*ibid*.).
>
> This sort of private information falls at the very heart of the "biographical core" protected by s. 8 of the *Charter*.[250]

The correlation between biographical core information and a reasonable expectation of privacy is made obvious. When addressing the biographical core, it is significant to note that the Court was clearly considering all the uses of the laptop, not just the child pornography that was found. This is consistent with framing the issue in a neutral way. The SCC also presented the biographical core more as a continuum; instead of as either biographical core or not. As a search gets closer to the biographical core of information, the more likely the Court will recognize a reasonable expectation of privacy and, therefore, a constitutionally protected privacy interest.

3.4.2 The Totality of the Circumstances Test

Context is critical to every section 8 analysis. The SCC has often stressed the importance of context. In *Kang-Brown* Justice Deschamps stated "because the requirement of a reasonable

[249] *Cole*, para 2.
[250] *Cole*, paras 46-48.

expectation of privacy is a guiding principle under s. 8, the consideration of relevant contextual factors is an integral part of the s. 8 analysis".[251] As Justice Deschamps explained in *Gomboc*, "context is crucial" to any section 8 analysis.[252] In assessing the reasonableness of an expectation of privacy, the SCC looks to what it calls the "totality of the circumstances". Through its different manifestations, the SCC has repeatedly referenced the totality of the circumstances to set the particular factual context for the search and decide whether there is a reasonable expectation of privacy for each case. [253] This permits a fact specific determination within the flexible framework provided by section 8.

The phrase "totality of the circumstances" was first articulated by the SCC in relation to section 8 cases in the 1996 case of *Edwards*.[254] In that case, Edwards was convicted for possession for the purpose of tracking cocaine after police entered his girlfriend's apartment on suspicion that there may be crack cocaine inside. The question for the SCC was "What rights does an accused person have to challenge the admission of evidence obtained as a result of a search of a third party's premises?" The issue was whether the accused had standing to assert his rights under section 8 of the *Charter* with respect to the search of his girlfriend's apartment. The analysis of that issue included consideration of the accused's reasonable expectation of privacy. The SCC set out the principle as follows: "A reasonable expectation of privacy is to be determined on the basis of the totality of the circumstances" and went on to provide:

---

[251] *Kang-Brown*, para 142. Similar statements can be found in *Wong*, para 47, para 57 and 59; *Plant*, para 26; *Kang-Brown*, para 171; *Gomboc*, para 23; *Marakah*, para 115.
[252] *Gomboc*, para 23. See also Justice Lamer's dissent in *Wong*; In *Spencer* SCC, Justice Cromwell for the Court explained that the analysis is "sensitive to the factual context", at para 18; Justice Moldaver in his dissent in *Marakah* provided that the reasonable expectation of privacy analysis is "context driven", beginning at para 115.
[253] Stuart, page 308. See *Tessling*, paras 31-32; *Edwards*, para 45; *Spencer*, para 18.
[254] The *Edwards* judgement refers back to *Wong* for the principle of totality of circumstances. *Wong* mentioned "in the circumstances" but did not develop "totality of the circumstances" nor factors for consideration.

> The factors to be considered in assessing the totality of the circumstances may include, but are not restricted to, the following: (i) presence at the time of the search; (ii) possession or control of the property or place searched; (iii) ownership of the property or place; (iv) historical use of the property or item; (v) the ability to regulate access, including the right to admit or exclude others from the place; (vi) the existence of a subjective expectation of privacy; and vii) the objective reasonableness of the expectation.[255]

This list of factors provided useful criteria for assessing the reasonableness of one's privacy expectations. Eleven years later, in *Tessling*, the SCC adapted the totality of the circumstances test from *Edwards* to the circumstances of that case. Justice Binnie for a unanimous court explained the use of this test as follows:

> I will proceed on the basis of the "totality of the circumstances" test set out by Cory J. in *Edwards* and the questions listed therein, at para. 45, but the questions need to be tailored to the circumstances of the present case.
>
> (1) Did the Respondent Have a Reasonable Expectation of Privacy?
>
> On the facts of this case, we need to address:
>
> 1. What was the subject matter of the FLIR image?
> 2. Did the respondent have a direct interest in the subject matter of the FLIR image?
> 3. Did the respondent have a *subjective* expectation of privacy in the subject matter of the FLIR image?
> 4. If so, was the expectation *objectively* reasonable? In this respect, regard must be had to:
>
> 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;

[255] *Edwards*, para 45.

> g. whether the FLIR heat profile exposed any intimate details of the respondent's lifestyle, or information of a biographical nature.[256]

After reviewing each of these factors, the judgement concluded that the accused had no reasonable expectation of privacy in information about patterns of heat distribution on the external surfaces of his home.[257]

This totality of the circumstances test was employed in *Kang-Brown* by Justice Deschamps in her reasons for judgement. Her restatement of factors reads:

> To determine whether the accused had a reasonable expectation of privacy, the totality of the circumstances must be considered. The accused must establish both an objective and a subjective expectation of privacy. In *Edwards*, at para. 45, and *Tessling*, at para. 32, this Court developed a non-exhaustive list of factors to assist in making this determination. The factors for determining whether the accused had a reasonable expectation of privacy may be summarized as including:
>
> (i) the presence of the accused at the time of the alleged search;
>
> (ii) the subject matter of the alleged search:
>
> (a) ownership and historical use of the subject matter;
>
> (b) whether the subject matter was in public view;
>
> (c) whether the subject matter had been abandoned;
>
> (d) where the subject matter is information, whether the information was already in the hands of third parties; if so, was there a duty of confidentiality in relation to it?
>
> (iii) the place where the alleged search occurred:
>
> (a) ownership, possession, control or use of the place where the alleged search took place;
>
> (b) the ability to regulate access, including the right to admit or exclude others from the place;
>
> (c) notification of the possibility of searches being conducted in the place;
>
> (iv) the investigative technique used in the alleged search:
>
> (a) whether the police technique was intrusive in relation to the alleged privacy interest;

[256] *Tessling*, paras 31-32.
[257] *Tessling*, para 63.

> (b) whether the information obtained in the alleged search exposed any intimate details of the accused's lifestyle, or information of a biographical nature.
>
> As in any contextual analysis, not all the factors will be relevant in a given case. The purpose of setting out a non-exhaustive list of factors stated in general terms is not to have each one considered slavishly regardless of materiality to the specific case, but to provide a helpful guide to ensure that relevant factors are not disregarded.
>
> In my view, because the requirement of a reasonable expectation of privacy is a guiding principle under s. 8, the consideration of relevant contextual factors is an integral part of the s. 8 analysis.[258]

It is interesting to note that this list of factors from *Kang-Brown* is not an exact copy of either previous list provided in *Edwards* or *Tessling*. Justice Bastarache also asserts that "[e]stablishing the existence of a reasonable expectation of privacy requires an assessment of the "totality of the circumstances" … and the specific factors to be considered must be tailored to the particular case".[259] Because the test requires tailoring, one should expect some fluidity in the listing of particular factors for each case. As Justice Binnie explained in *M(A)*, "s. 8 jurisprudence will continue to evolve as snooping technology advances. This flexibility is essentially what the "totality of the circumstances" approach is designed to achieve."[260]

In *Patrick*, the SCC used the totality of the circumstances as an analytical framework, structuring the judgement around the *Tessling* factors.[261] In *Gomboc*, Justice Deschamps' reasons for judgement were dependent on the totality of the circumstances.[262] Justice Abella in her concurring reasons and Justice McLachlin in dissent both also relied on the totality of circumstances. Justice Abella simplified the factors as follows:

---

[258] *Kang-Brown*, paras 140-142. Justice Deschamps uses the same list in *M(A),* para 128.
[259] *Kang-Brown*, para 226.
[260] *M(A)*, para 40.
[261] *Patrick*, beginning at para 26.
[262] *Gomboc*, paras 2, 23 and 34.

> … the subject matter of the information sought, whether the individual had a direct interest in this subject matter, whether the individual had a subjective expectation of privacy in the subject matter, and whether such an expectation of privacy in the subject matter was also objectively reasonable.[263]

She then says the final inquiry regarding an objectively reasonable expectation of privacy, "may entail consideration of a wide array of relevant factors".[264] This particular reiteration of the totality of the circumstances has since become the preferred version of the framework. For example, in *Cole*, Justice Fish for the majority provided:

> The "totality of the circumstances" test is one of substance, not of form. Four lines of inquiry guide the application of the test: (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.[265]

The same four headings were used consistently by the SCC since *Cole* as can be seen in *Spencer*,[266] *Jones*[267] and *Marakah*.[268] These four factors are essentially a return to the *Tessling* factors but without a listing of all the potential sub-factors under the fourth.

3.5 CONCLUSION

Section 8 of the *Charter* is intended to restrain government action and protect individuals from unreasonable searches or seizures. The SCC's approach to section 8 cases seems fairly straightforward based on the above review – it is a normative inquiry to balance values using

[263] *Gomboc*, para 78.
[264] *Gomboc*, para 78.
[265] *Cole*, para 40.
[266] *Spencer* SCC. para 18.
[267] *Jones*, para 13.
[268] *Marakah*, para 11.

analytical tools created for that purpose. Informational privacy is recognized as a distinct sphere of privacy. The purpose of section 8 is to prevent unjustified state intrusion on individual's reasonable expectations of privacy. The reasonable expectation of privacy analysis looks at what information ought to be protected. The SCC has explicitly rejected a risk analysis approach to privacy. If a privacy interest is identified, the SCC then turns to a balancing of the individual privacy interest with the State's interest in the intrusion.

The SCC has identified that a biographical core of personal information is protected by section 8. They have used this tool of analysis at different points throughout section 8 jurisprudence. The Court has created a test to assess the reasonableness of any expectation of privacy, called the totality of the circumstances. This test is meant to provide a contextual and flexible framework. While the framework has been articulated in different ways throughout the cases, the four factors as set out in *Cole* have remained consistent.

Now that the foundational principles have been outlined, chapter 4 can take a deeper and more critical look at the Court's approach to informational privacy through section 8 of the *Charter* and addresses challenges it presents.

CHAPTER 4: CHALLENGES WITH THE CURRENT INTERPRETATION OF SECTION 8 OF THE *CHARTER*

4.1 INTRODUCTION

Now that this thesis has explored what the law is, this chapter attempts to explain why there are problems with the current state of section 8 jurisprudence and why the line between lawful and unlawful searches of technology is so difficult to draw. I identify three specific issues with the interpretation of section 8 with a view to examining the major challenges to achieving certainty. The three issues reviewed in this chapter are: 1. Conceptual incompatibility between a stated normative approach and the analytical tools employed, 2. Uncertainty prevalent in the jurisprudence and 3. Relevant legislation.

Chapter 4 begins in section 4.2 explaining a foundational disconnect between the Court's normative approach and the positive analytical tools designed to assess a reasonable expectation of privacy. This conceptual issue is discussed as the first challenge with the current interpretation of section 8 of the *Charter* because it is central to all section 8 inquiries. The tools of analysis introduced in chapter 3, section 3.4 – the biographical core and totality of the circumstances – are positive, not normative. Section 4.2 explains how the normative privacy analysis gets confused when approached with these factual inquiries. The cases of *Spencer* and *Marakah* are used to demonstrate this point. In *Spencer*, the key element of the totality of the circumstances test – the subject matter of the search – adds significant confusion to the already problematic analysis. *Marakah* is used to demonstrate how the SCC focuses their attention on the positive indicators of a reasonable expectation of privacy instead of conducting a normative analysis. A review of the incompatibility shows that the core concern underlying all search and seizures cases is actually dignity, which will be significant when I explore possible solutions to the challenges of section 8 in chapter 5.

In addition to the foundational conceptual issue, in section 4.3 I discuss some practical and more discrete problems of uncertainty with the jurisprudence. The SCC contributes to an uncertainty in section 8 through an inconsistent application of principles. The biographical core is discussed in this section. While section 3.4 introduced the concept, section 4.3 explains how the SCC has been inconsistent in its application; not only with when it is used, but what is included within the biographical core. By using an ad hoc approach, leaving caveats within their judgments and rendering split decisions, the SCC has left confusion in an area of the law that is meant to prevent unjustified searches. Each of these ideas is explored within section 4.3.

To complete this chapter on the challenges with the current interpretation of section 8, section 4.4 discusses how out of date legislation contributes to the problem of keeping pace with searches of technology. Lastly, section 4.5 uses the *Mills* case as a demonstration of the challenges identified within this chapter. Given the issues identified in this chapter, it should not be surprising that there is no authoritative answer to my research question.

4.2 CONCEPTUAL INCOMPATIBILITY: A NORMATIVE APPROACH AND THE ANALYTICAL TOOLS

4.2.1 The Incompatibility Explained

As outlined in chapter 3, section 3.2, the SCC has consistently held that a section 8 inquiry into whether a person has an expectation of privacy "is a normative rather than descriptive

standard".[269] The Court asks what information *ought to be* protected by section 8, not whether it *actually* is protected.[270]

A normative approach addressed with positive tools creates a logical disconnect because the two concepts are fundamentally different. A normative statement expresses a value judgment about whether a situation is desirable or undesirable. Normative statements characteristically contain verbs such as "should" or "ought to". A normative question is one that asks, "what should be", which logically produces a subjective response. Normative statements are the opposite of positive statements. Positive statements are objective statements that can be tested or rejected by referring to evidence or facts. A positive question would ask instead "what is".[271]

Instead of applying normative tools to the purportedly normative section 8 analysis, the SCC have employed primarily positive analytical tools – the biographical core and totality of the circumstances. Looking back to chapter 3, section 3.4, we know that the SCC considers section 8 to protect a biographical core of personal information, including information which tends to reveal intimate details of lifestyle and personal choices and which individuals would wish to maintain and control from disclosure to the State. Whether information is part of one's biographical core seems as though it would be primarily an objectively measurable device; with information being either part of or not part of a biographical core. However, this seemingly factual question is not

[269] *Tessling*, para 42. Note, the term "normative" is not judicially defined.
[270] See *Spencer* SCC, para 18. For example, in *Dyment*, police *actually* got his blood from the doctor, but the SCC found he *should* have maintained privacy in it. In *Wong* police *actually* were able to gain access to the hotel room, but the majority of the SCC held he maintained a reasonable expectation of privacy because people who retire to their hotel room and close the door *should* have privacy. In *R v Law,* 2002 SCC 10, [2002] 1 SCR 227 [*Law*], police *actually* had access to the contents of the stolen safe, but the Court held Law *should* be able to continue to expect privacy. These cases establish that just because privacy is not *actual* realized privacy, does not mean section 8 will not protect the privacy interest.
[271] For more reading on normative versus positive statements and ideas, see Philip Soper, "Legal Systems, Normative Systems, and the Paradoxes of Positivism" (1995) 8 Can J L & Juris 363.

easy to apply and contains a normative element (would wish to) within its definition. As will be discussed in section 4.3.2 below, the SCC has been inconsistent in the application of the biographical core to section 8 cases.

In determining whether there is a reasonable expectation of privacy in the totality of the circumstances the Court has provided factors to consider, including: (i) the accused's presence at the time of the search, (ii) ownership, possession, control and historical use of the subject matter of the search or the place of the search, (iii) whether the subject matter was in public view or abandoned, (iv) whether the information was already in the hands of third parties. These are all positive, factual and mostly binary questions. When considering searches of technology for information these factors do not consider the relevant issues of privacy. For example, a person will almost never be present at the time of a database search as the server containing the information is likely in a physical location outside of the individual's province or even State.[272] Individual's do not have ownership, possession or control over the servers or the information, which are by their nature in the hands of third parties – usually a corporation. Such an approach to informational privacy questions is puzzling when part of a broad and purposive interpretation. These factors in the totality of the circumstances test create a sterile review of the facts and miss the real concerns of protecting information that ought to be protected and preventing unjustified searches of that information. It is practically easier to employ these tools because they are objectively measurable. However, the language used does not reflect or match what the Court intends to do, nor does it address the real concerns of section 8 that genuinely motivate them,

[272] For example, audio interactions with Alexa are sent to the Cloud: https://www.amazon.com/gp/help/customer/display.html?nodeId= 201602230.

which will be discussed in detail below after the examples. This incongruity makes it difficult to predict how the Court will apply section 8 considerations to emerging technology.

4.2.2 Examples of the Incompatibility

This incompatibility is prominently displayed in recent cases from the SCC dealing with section 8 in the context of technology: *Spencer* and *Marakah*. I will outline these cases in detail to demonstrate the incompatibly described above and also to show issues with the Court's approach to section 8 in technology cases. The *Spencer* judgment demonstrates that, within the already problematic totality of the circumstances test, the defining of the subject matter of the search often has a controlling interest in determining the result of the analysis. The *Marakah* judgment demonstrates how the SCC has attempted to use factual considerations within the totality of the circumstances analysis.

Spencer

In *Spencer*, police discovered child pornography in a shared folder on LimeWire, an online file sharing program.[273] LimeWire displayed the account user's Internet Protocol (IP) address[274] to other users as part of the file sharing process.[275] Police did not know who was using the account or where the computer was located. To link the IP address to a person and location, investigators made a request to the Internet Service Provider (ISP) Shaw Communications (Shaw) for the name,

[273] *R v Spencer*, 2011 SKCA 144, [2011] 377 Sask R 280 [*Spencer* SKCA], see para 5 for explanation of how the file sharing program functioned.
[274] See *Ward*, at paras 21-22, "IP address is a unique multi-digit numerical identifier that is automatically and randomly assigned by an ISP to a subscriber when the subscriber's computer device connects to the Internet." An IP address is something that belongs to and is controlled by the ISP at all times. It is, in effect, loaned to individuals to use so that they may connect to the internet. An IP address says nothing more than that an individual has an internet connection. IP information is useless without prior and subsequent investigation. "Subscriber information" is the customer information – name, address, phone number – of the person using the ISP's services. It is evidence of a contractual relationship for an internet connection.
[275] *Spencer* SCC, para 8.

address, and phone number of the IP address account holder as of August 31, 2007 at 1246 hours.[276] Shaw provided the requested information which police used to obtain a search warrant for the physical address associated with the IP address. When police executed the search warrant they found 441 distinct images and 112 videos of child pornography downloaded on Mr. Spencer's computer and in its shared folder.[277] They also learned that Spencer was not the Shaw subscriber; that was Spencer's sister, with whom Mr. Spencer resided. Mr. Spencer was identified as the LimeWire account user and he was charged with possession of child pornography and making it available to others through the internet.[278]

Spencer applied to have the evidence obtained as a result of the police obtaining the subscriber information matching the IP address from Shaw excluded from his trial based on a violation of his section 8 *Charter* rights. Spencer's position was that police obtained the IP address from Shaw without a warrant, making their actions an unreasonable search and seizure.[279]

In assessing Spencer's application, Justice Foley at the Saskatchewan Court of Queen's Bench reviewed the concept of reasonableness and held that "there is neither objective nor subjective expectations of privacy in a subscriber's name and address relating to the IP address issued by the internet service".[280] Consequently, there was no search and no *Charter* breach. Spencer was convicted of possession of child pornography and acquitted of making child

[276] *R v Spencer*, 2009 SKQB 341, [2009] 361 Sask R 1 [*Spencer* SKQB], paras 9-11; and *Spencer* SKCA, para 7.
[277] *Spencer* SKCA, para 9.
[278] *Spencer* SKQB, para 1.
[279] *Spencer* SKCA, at para 11.
[280] *Spencer* SKQB, at paras 18 and 32.

pornography available. Both Spencer and the Crown appealed that decision.[281] Spencer argued that the trial judge erred in finding he had no reasonable expectation of privacy.[282]

The Court of Appeal found that because "Spencer was using his computer inside his home to access child pornography, Mr. Spencer undoubtedly held a subjective expectation of privacy in the Disclosed Information; but was his expectation objectively reasonable, having regard to the totality of the circumstances?"[283] Justice Caldwell defined the subject matter of the search more broadly than Justice Foley based on its potential to reveal "intimate details of lifestyle and personal choices of Mr. Spencer, and his activities within his home".[284] The court considered the terms of the Service Agreement with Shaw as "relevant and material" to Spencer's claim in having a reasonable expectation of privacy.[285] The terms of the policy made Spencer's expectation of privacy unreasonable.[286] Using these positive factors, the Court of Appeal held that there was no search in violation of section 8 of the Charter, even if there had been a search, it was reasonable "in all respects" and did not violate the Charter.[287] His appeal was dismissed. They also found the trial judge erred in considering the *mens rea* of making child pornography available to others and ordered a new trial on that charge.[288]

In separate reasons, concurring in result, Justice Ottenbreit did not agree with Justice Caldwell's characterization of the subject matter of the search. He explained:

> In my view, the Disclosed Information in this case merely establishes the identity of the contractual user of the IP address, who in this case was not the accused. The

[281] *Spencer* SKCA, at para 2.
[282] *Spencer* SKCA, at para 12.
[283] *Spencer* SKCA, at para 17.
[284] *Spencer* SKCA, at para 22.
[285] *Spencer* SKCA, at para 33, see paras 28-31.
[286] *Spencer* SKCA, at paras 33 and 46.
[287] *Spencer* SKCA at para 47.
[288] *Spencer* SKCA, at paras 93 and 95.

> *potential* that the Disclosed Information might in this case *eventually* reveal much about the individual and the individual's activity is, in my view, neither here nor there.[289]

Justice Ottenbreit's definition of the subject matter of the search as "name, address and telephone number" is the same as the trial judge's.[290] Containment of the subject matter of the offence to simply name, address and phone number influences the assessment and is important to the analysis.

The lower court decisions in *Spencer* reflect a larger uncertainty around how to characterize the link to a name and address in the context of online activity. Spencer's appeal to the SCC allowed our highest court to provide clear direction on this controversial issue. The fact that there were six interveners to the appeal demonstrate the significance of the outcome and its predicted ramifications.[291]

It is important to review the positions of the parties and the interveners before examining the judgment of the SCC to see how they tried to use measurable factors to make a normative assessment. This background places the decision in context to understand the legal landscape at the time just before *Spencer* was released. At the Supreme Court of Canada, Spencer argued:

> The fundamental error committed by Caldwell, J.A. was to not appreciate the significant impact of the disclosure of the subscriber information attached to an IP address on one's privacy rights. The Internet has created an unusual situation where one can obtain a great deal of information about a particular user without identifying that individual. The individual's privacy rights are protected by anonymity. Once the individual's identity is provided his/her privacy rights are significantly infringed.[292]

---

[289] *Spencer* SKCA, at para 110.
[290] *Spencer* SKQB, at para 18.
[291] Interveners: Director of Public Prosecutions, Attorney General of Ontario, Attorney General of Alberta, Privacy Commissioner of Canada, Canadian Civil Liberties Association, Criminal Lawyers' Association of Ontario.
[292] Factum of Appellant, para 39 [Factum of Appellant].

His argument continued: "[t]he error of the Court of Appeal wasn't that it applied the wrong test but rather that it failed to appreciate the applicability of that test to online technology which challenges our conventional concepts of possession and privacy."[293]

In response, the Crown argued that Spencer's view of privacy was far too expansive and went beyond the actual search that occurred. The Crown's position, as outlined in their factum, provided:

> To find a reasonable expectation of privacy in such information simply because it has the potential, when combined with other information, to reveal deeper truths about us, would cloak essentially everything in privacy. Search warrants would be required for most every policy inquiry and other citizens and corporate citizens would be improperly constrained from helping with law enforcement. That is neither true to the 'balancing' which underlies s. 8, nor workable.[294]

The two parties to this litigation took very different approaches to the subject matter of the search. Spencer's position was that the Court should look at the implications of identifying a person through their IP address while the Crown's view was much more limited.

Before reviewing the judgement of the SCC, it is worthwhile to review the positions of the interveners to see how this positive versus normative disconnect is apparent. Their viewpoints were influential to the judgment and demonstrate the disagreement on the larger issues of privacy in online activity. The Attorney General of Ontario premised its argument from a narrow approach to the subject matter of the search:

> In this case, the details the police requested from Shaw Communications were a name and an address connected to an Internet Protocol (IP) address associated to child pornography at one point in time. …. Under the direction of this Court's strong line of cases from *R. v. Plant* to *R. v. Cole*, the proper analysis of the s. 8 claim should focus on the nature of the information obtained, and the details that it alone provides. The sheet faxed by Shaw Communications did not reveal

[293] Factum of Appellant, at para 45.
[294] Factum of Respondent – Her Majesty the Queen, para 45 [Factum of Respondent].

> information tending to expose the appellant's intimate biographical details: it did not identify the appellant at all. That should end the matter.[295]

The Attorney General of Ontario resorted to the biographical core of information and tried to say that because the information at issue did not expose a biographical core of information it did not fall within section 8 protection. This is a very positivist approach to the question, using facts to determine the correct outcome.

The Attorney General for Alberta and the Director of Public Prosecutions took the same position as the Attorney General for Ontario.[296] Both Crown Interveners expressed serious concerns to an approach that would recognize the police request to Shaw as being a search. As the Attorney General for Alberta expressed:

> If asking an internet service provider (ISP) for customer name and address is a search, then so is virtually every other inquiry made of an institutional witness. To characterize this routine police inquiry as a "search" would be a major departure from existing jurisprudence, with unacceptable consequences for law enforcement.[297]
> …
>
> If seeking trivial information from a commercial organization is an unreasonable search, the consequences for policing and prosecution will be dire.[298]
> …
>
> If a warrant is required in the case at bar, warrants would likely also be required in the above scenarios and countless others. The implications for police and court resources are obvious.[299]

The Crown was concerned about the broader implications for police investigations if this case was to expand the right to privacy provided under section 8 of the *Charter*. The Director of Public Prosecutions warned the Court of the potential consequences of their decision:

---

[295] Factum of Intervener – Attorney General of Ontario, paras 5-6 [Factum of AG Ontario].
[296] See Factum of Intervener – Attorney General of Alberta, paras 3 and 24 [Factum of AG Alberta; and see Factum of Intervener – Director of Public Prosecutions, at para 2 [Factum of DPP].
[297] Factum of AG Alberta, para 3.
[298] Factum of AG Alberta, para 24.
[299] Factum of AG Alberta, para 25.

> It takes little imagination to realize that a right to use the publicly accessible segment of the Internet anonymously would make the Internet even more crime-friendly.[300]
>
> Recognition of a general right to interact anonymously in public is simply incompatible with society's more compelling interest in protection and security.[301]
>
> The proscription against identification flowing from the appellant's proposed right of anonymity must be so broad as to preclude police from even receiving clues toward identification without a warrant. The breadth of the novel right of anonymity claimed here evinces an attempt to use the *Charter* to advance conditions most favorable to criminality.[302]

The Crown was concerned about what a right to anonymity could mean for crime prevention and enforcement. This approach is framed in a normative way – the information *should* not be protected because of broader public policy and security reasons.

The Interveners in support of Spencer's position were the Privacy Commissioner of Canada, the Criminal Lawyers' Association of Ontario and the Canadian Civil Liberties Association. They all argued that there is a reasonable expectation of privacy in subscriber information because it can in fact provide intimate details of an individual's online activities.[303] These interveners describe the privacy interest from the broader perspective of the potential consequences of the search rather than the actual results of the search.[304] Instead of conducting the analysis based on the subscriber information of name, address and telephone number, the Canadian Civil Liberties Association argued:

> Internet browsing and surfing activities tend to reveal intimate details about a person's lifestyle and personal choices such that the consequences of lifting the anonymity provided by an IP address are profound and widespread. As a result, such information is subject to a reasonable expectation of privacy and the protection of section 8 of the *Charter*. Because piercing the anonymity supplied by an IP

[300] Factum of DPP, at para 22; see also para 18.
[301] Factum of DPP, at para 24.
[302] Factum of DPP, at para 28.
[303] Factum of Intervener – Privacy Commissioner of Canada, at paras 5 [Factum of PCC]; Factum of Intervener – Canadian Civil Liberties Association, at paras 1 and 5 [Factum of CCLA].
[304] Factum PCC, at para 18.

> address is the key to connecting an individual to their online activities, the CCLA submits that section 8 of the *Charter* is engaged by such an intrusion.[305]

This approach relies on privacy protection through resorting to the biographical core analysis. The Criminal Lawyers' Association of Ontario advanced their argument from a similar starting position:

> Someone armed with this information can easily learn details of a person's activities on the internet, which can be extremely revealing. Access to this information should therefore be judicially regulated under s. 8 and the police should not be able to obtain it without a warrant.[306]

These interveners advocated for a recognition of the right to anonymity based on the fact that the information can be revealing; claiming it was essential to ensuring privacy online.[307] This is still a positive approach looking to the factual and measurable activities at issue.

One theme stands out from a reading of the factums of the parties and interveners – the recognition of the significance of this case. The Canadian Civil Liberties Association started their factum with the statement that the "implications of this appeal are profound" since "the case has much broader policy implications".[308] The Criminal Lawyers' Association of Ontario also noted that this "is a watershed moment for the right to privacy".[309] The idea that this case would have such a major impact was palpable. Either the Court would find there was a reasonable expectation of privacy or not. There was no middle ground that would make all the parties happy given their "markedly divergent perspectives" on defining the subject matter of the search.[310]

---

[305] Factum of CCLA at para 2.
[306] Factum of Intervener – Criminal Lawyers' Association of Ontario, at para 2 [Factum of CLAO].
[307] Factum of CCLA, at paras 2, 7 and 10.
[308] Factum of CCLA, at para 1.
[309] Factum of CLAO, at para 3.
[310] *Spencer* SCC, para 23.

The oral arguments of each party presented at the Supreme Court of Canada focused on defining the subject matter of search as part of the totality of the circumstances test.[311] Justices LeBel expressed concerns about burying our heads in the sand on the potential information available to police through an IP address. Justice Moldaver expressed concern with the Crown's "narrow and formalist view" of the subject matter of the search. The consistent message from the bench during the hearing was a fear of the breadth of information available from an IP address. The Justices were obviously troubled by the possibility of substantial intrusions into one's online activity that technology permits more generally.

On June 13, 2014 the Supreme Court of Canada released its decision in *Spencer*.[312] Justice Cromwell, writing for the unanimous court, started the reasons for judgment with the statement that "The Internet raises a host of new and challenging questions about privacy. This appeal relates to one of them."[313] The Court determined that the accused had a reasonable expectation of privacy in the subscriber information for his sister's Internet Protocol (IP) address. In considering the totality of the circumstances to determine whether there was a reasonable expectation of privacy, and ultimately whether there was a search, the subject matter of the search was defined broadly as "the identity of a subscriber whose Internet connection is linked to particular, monitored Internet activity".[314] The judgment then discusses the "nature of the privacy interest potentially compromised by the state action".[315] Justice Cromwell explained:

> The Court has previously emphasized an understanding of informational privacy as confidentiality and control of the use of intimate information about oneself. In my view, a somewhat broader understanding of the privacy interest at stake in this case

[311] See *Supreme Court of Canada Webcast* for File 34633, online: http://www.scc-csc.ca/case-dossier/info/webcastview-webdiffusionvue-eng.aspx?cas=34644&id=2013/2013-12-09--34644&date=2013-12-09&fp=n&audio=n.
[312] *Spencer* SCC.
[313] *Spencer* SCC, at para 1.
[314] *Spencer* SCC, at paras 32-33.
[315] *Spencer* SCC, beginning at para 34.

> is required to account for the role that anonymity plays in protecting privacy interests online.[316]

This is the first indication that the Supreme Court of Canada may recognize anonymity as a part of informational privacy protections. The judgment went on to provide that informational privacy includes "privacy as secrecy, privacy as control and privacy as anonymity".[317] Justice Cromwell discussed the idea of privacy as anonymity in the context of internet usage and explained that "anonymity may, depending on the totality of the circumstances, be the foundation of a privacy interest that engages constitutional protection against unreasonable search and seizure."[318] The decision holds that "the police request to Shaw for subscriber information corresponding to specifically observed, anonymous Internet activity engages a high level of informational privacy."[319] The Court explicitly recognized anonymity as "an important safeguard for privacy interests online".[320] The subscriber information was unconstitutionally obtained and therefore the search of the residence, based on that information, was unlawful and violated section 8 of the *Charter*.[321] Ultimately, the evidence was not excluded under section 24(2) since admission of the evidence would not bring the administration of justice into disrepute; the conviction for possession of child pornography was affirmed with the count of making child pornography available being sent back for a new trial.[322]

---

[316] *Spencer* SCC, at para 34.
[317] *Spencer* SCC, at para 38.
[318] *Spencer* SCC, at para 48.
[319] *Spencer* SCC, at para 51.
[320] *Spencer* SCC, at para 78.
[321] *Spencer* SCC, at para 74.
[322] After the Supreme Court of Canada decision, the matter was sent back to the Saskatchewan Court of Queen's bench where Spencer was found guilty of making child pornography available through the internet (*R v Spencer*, 2015 SKQB 62, [2015] 469 Sask R 64). Spencer successfully appealed that conviction. The Court of Appeal ordered a stay of proceedings because they found that the trial judge's reasons for conviction were not sufficient for appellate review and that sending the matter back for a third trial would amount to an abuse of process (*R v Spencer*, 2017 SKCA 54, [2017] SJ No 282, at paras 10, 93, 126 and 128).

As set out earlier, on a section 8 application, a court must consider whether there is a reasonable expectation of privacy in the totality of the circumstances with reference to: (1) the *subject matter* of the search; (2) the claimant's interest in the *subject matter*; (3) the claimant's subjective expectation of privacy in the *subject matter*; and (4) whether this subjective expectation of privacy was objectively reasonable, having regard to the totality of the circumstances.[323] The "subject matter" of the search is central to the determination on a section 8 application. The framing of the subject matter of the search informs the entire analysis and heavily influences the result of the inquiry. It is problematic if the subject matter of the search is too narrowly defined or too widely defined. In *Spencer*, the search at issue could have been defined as "a name and address of someone in a contractual relationship with Shaw."[324] A name, address and telephone number do not disclose intimate details giving rise to a heightened level of privacy protection. The Court defined the subject matter of the search as "the identity of a subscriber whose Internet connection is linked to particular, monitored Internet activity".[325] By defining the subject matter as a gateway to online activity, it attracted an expectation of privacy, and thus was a search within the meaning of section 8. The same discussion was addressed in relation to the more recent case of *Marakah*, which will be discussed in detail next. As one of the counsel from that case expressed:

> This sort of context-specific analysis, which argued in favour of a reasonable expectation of privacy in sent text messages, flowed directly from the way McLachlin CJ characterized the issue at the outset of her analysis. The defense essentially won the case when it won the issue-framing contest.[326]

[323] *Spencer* SCC, at para 18.
[324] *Spencer* SCC, at para 32.
[325] *Spencer* SCC, at para 33.
[326] Gerald Chan, "Test Messaging: The Most Private (And Recorded) Form of Communication" (2018) 36 Adv J No. 4, at para 12. Note, Gerald Chan was co-counsel to the British Columbia Civil Liberties Association in *Marakah* and *Jones*.

As Justice Cote expressed in *Jones*, properly defining the subject matter is "vital".[327] Different courts and parties strongly disagree on this underlying premise. The divergent perspectives of the parties to the *Spencer* case are an indication that the subject matter of the search, a part of the totality of the circumstances test, has an inflated controlling interest in the result and adds to the argument that the totality of the circumstances may not be the best analytical tool to use for technology search cases. The Court in *Spencer* intended to answer the question of whether persons *should* have privacy protection in their online activities including their association with an IP address. Underlying the Court's judgement is really the intention to protect a sphere of privacy in our internet activity that allows for autonomy and freedom of expression.

Marakah

The SCC spent time in *Marakah* discussing the significance of control over information in the section 8 analysis. In that case, Marakah had sent his accomplice incriminating text messages about their illegal firearms transaction. The smartphones of Marakah and his accomplice were seized by police and searched. The trial judge found that the search of Marakah's home was invalid and text messages from his smartphone could not be used against him. The question arose as to whether the Crown could use the text messages recovered from his accomplice's device, which had also been obtained through an unlawful search.[328] The trial judge answered this question in the affirmative, finding Marakah had no standing with respect to the text messages on the other's device. The texts were admitted into evidence and Marakah was convicted. On appeal, the Court

[327] *Jones*, para 14.
[328] *Marakah*, para 62.

of Appeal found there was no reasonable expectation of privacy in sent text messages and Marakah had no standing to argue admissibility.

The question for the SCC was whether there was a reasonable expectation of privacy in messages sent to another person and whether Marakah could claim section 8 *Charter* protection for text messages accessed through his accomplice's smartphone. The Crown conceded that if the SCC found that Marakah had standing, the search was unreasonable and a violation of section 8. A majority of the SCC allowed the appeal, set aside the convictions and entered an acquittal. Chief Justice McLachlin writing for the majority found that Marakah subjectively believed his texts to be private and that expectation of privacy was objectively reasonable.[329]

As pointed out by Justice Rowe, concurring in separate reasons with Chief McLachlin's majority, the disagreement on the Court in *Marakah* was about the importance of control in the reasonable expectation of privacy analysis.[330] Chief Justice McLachlin for the majority stated that "control is not an absolute indicator of a reasonable expectation of privacy, nor is lack of control fatal to a privacy interest".[331] She explained:

> Control is one element to be considered in the totality of the circumstances in determining the objective reasonableness of a subjective expectation of privacy. Control must be analyzed in relation to the subject matter of the search: the electronic conversation. Individuals exercise meaningful control over the information they send by text message by making choices about how, when, and to whom they disclose the information.[332]

Justice Moldaver in dissent asserted control as a crucial factor.[333] He explained his position as follows:

---

[329] *Marakah*, para 6. In coming to that result, she determined that the subject matter of the search was the electronic conversation, not only the copy of the message as stored on the device or server.
[330] *Marakah*, para 85.
[331] *Marakah*, para 38.
[332] *Marakah*, para 38-39.
[333] *Marakah*, para 98.

> Here, Mr. Marakah had no control whatsoever over the text message conversations on Mr. Winchester's phone. Mr. Winchester had complete autonomy over those conversations. He was free to disclose them to anyone he wished, at any time, and for any purpose. To say that Mr. Marakah had a reasonable expectation of personal privacy in the text message conversations despite his total lack of control over them severs the interconnected relationship between privacy and control that has long formed part of our s. 8 jurisprudence. It is equally at odds with the fundamental principle that individuals can and will share information as they see fit in a free and democratic society.[334]

Moldaver felt that the majority's approach "threatens a sweeping expansion of section 8 standing"[335] and risks "disrupting the delicate balance".[336] He concluded that Marakah had no control and therefore no reasonable expectation of privacy in the subject matter of the search.[337] Even the parties focused at least some of their attention on these positive indicators of a reasonable expectation of privacy, instead of conducting a normative analysis. The Crown argued that Marakah lost control over the text message conversation.[338]

Whether someone maintains control over information at issue should not be a consideration at all on a normative approach to section 8. On a normative inquiry, the question in *Marakah* is whether people *should* be able to expect privacy in their text message conversations. The SCC was actually concerned with the State gaining access to our personal text message conversations without the proper authorization. On a normative analysis, control would not be a factor for determining whether there should be privacy protections. Even if a person factually has a total lack of control (such as in their data being held by a corporation) does not mean they cannot expect any privacy protections.

---

[334] *Marakah*, para 99.
[335] *Marakah*, para 100.
[336] *Marakah*, para 114.
[337] *Marakah*, paras 145, 147.
[338] *Marakah*, para 40.

Marakah demonstrates that even when the SCC employs a positive question – such as whether the accused had control over the information – the Justices disagree on the answer. They are using the terminology of control but are actually concerned with whether privacy protection *should* extend to text messages in a normative way. The confusion caused by this disconnect will be exacerbated when it comes to technology because the boundaries between lawful and unlawful are even harder to define.

In both *Spencer* and *Marakah* it is easy to see the normative intention underlying the analysis, but the positive analytical tools do not adequately achieve the purpose of section 8. This is why the Court faces difficulty in maintaining clarity and predictability. Unless the Court starts to shift the discourse to reflect the real concerns of section 8, confusion will continue.

4.2.3 Dignity: The Core Concern of Section 8

The core concern underlying all search and seizures cases is dignity. The SCC has repeatedly recognized that the main aim of section 8 is to protect individual dignity. In *Dyment*, the SCC was concerned with the dignity of an individual when an agent of the State takes a person's blood without consent. Justice LaForest was clear that such a seizure was "a serious affront to human dignity".[339] He went on to reference the Task Force on Privacy and Computers as follows:

> …. this sense of [informational] privacy transcends the physical and is aimed essentially at protecting the dignity of the human person. Our persons are protected not so much against the physical search (the law gives physical protection in other ways) as against the indignity of the search, its invasion of the person in a moral sense.[340]

[339] *Dyment*, para 32.
[340] *Ibid*.

Again, he explained that "there is a privacy in relation to information. This too is based on the notion of dignity and integrity of the individual".[341] In *Plant*, Justice Sopinka for the majority also asserted that dignity is central to the purpose of section 8. As he explained, when the "dignity, integrity and autonomy of the individual are directly compromised", that is when the state has been found to run afoul of the section 8 right against unreasonable search and seizure.[342] He articulated the balancing within section 8 as being "societal interests in protecting individual dignity, integrity and autonomy with effective law enforcement".[343] In *Tessling*, in holding that there was no reasonable expectation of privacy in the heat patterns emanating from the home, Justice Binnie noted that its "disclosure scarcely affects the 'dignity, integrity and autonomy' of the person whose house is subject of the FLIR image".[344] In *Cole*, Justice Fish for the majority stated that in the context of a section 8 case, the focus is "on whether the search demeaned his or her dignity".[345]

In the case of *Fearon*, the SCC was asked to consider whether section 8 was violated in the search of a cell phone incident to arrest. Justice Cromwell for the majority set out new guidelines for the police to follow in searching a cell phone incident to arrest. He explained that such a search would be lawful if the arrest was lawful, the search of the cellphone was truly incidental to the arrest and there was a valid reason for the search. Since the police who searched Fearon's cell phone did not meet this threshold, Justice Cromwell found there to be a section 8 violation.[346] In her dissenting reasons, Justice Karakatsanis considered dignity as part of the analysis. She wrote:

> Our *Charter* jurisprudence recognizes the concept of a "sphere of privacy" to define the proper limits of state authority in a free and democratic society. It recognizes that privacy – a sphere of protection for private life – is essential to personal

[341] *Dyment*, para 33.
[342] *Plant*, para 24.
[343] *Plant*, para 26.
[344] *Tessling*, para 63.
[345] *Cole*, para 91.
[346] *Fearon*, para 88. Note the evidence was not excluded, in part because the jurisprudence was developing at in a "gray area", see paras 94-95.

> freedom and dignity …. Privacy gives us a safe zone in which to explore and develop our identities and our potential both as individuals and as participants in our society.[347]

In holding that the search was unreasonable and the evidence should be excluded she stated:

> The fact that a cell phone may keep and access meticulously taken records about almost every aspect of a person's life explains both why searching it would be so useful to law enforcement and why such a search may be so offensive to the person's dignity.[348]

The idea that dignity underlies section 8's purpose continues in the more recent cases of *Marakah*[349] and *Jones*.[350] Clearly, dignity informs the Court's analysis more than whether an accused maintains possession or control of the information and is present at the time of the search. The positive tools of analysis created to address section 8 cases do not address the normative underlying concern for dignity as expressed by the Court.

In addition to this foundational disconnect problem within section 8 jurisprudence, there is further uncertainty.

4.3 UNCERTAINTY WITHIN THE JURISPRUDENCE

This section reviews some practical and more concrete problems of uncertainty within the section 8 jurisprudence. In addition to the inherent uncertainty, inconsistency, caveats and split judgments leave confusion as a constant theme.

[347] *Fearon*, para 112, see also para 103.
[348] *Fearon*, para 145.
[349] See paras 53 and 179.
[350] See paras 29 and 38.

4.3.1 Uncertainty Inherent within Section 8

The SCC has repeatedly acknowledged that while the language of section 8 may be simple, it is inherently imprecise.[351] In one of the most contentious section 8 cases dealing with sniffer dog searches, Justice Binnie stated that "[s]ection 8 has proven to be one of the most elusive *Charter* provisions despite the apparent simplicity of its language".[352] *Hunter v Southam* recognized that the guarantee provided by section 8 is "vague and open".[353] This permits flexibility but at the cost of certainty.[354] The foundational analytical concept for any section 8 analysis is "a reasonable expectation of privacy". The phrase "unreasonable search and seizure" requires an understanding of "unreasonable". Yet, the meaning of the terms "unreasonable" and "reasonable" are open to a variety of valid, competing interpretations. What is "reasonable" changes over time. Privacy itself is a fluctuating concept.[355] These are extremely difficult terms to define with any precision.[356]

The concept of privacy is constantly evolving and has blurred "reasonableness" boundaries.[357] Privacy is a vague social construct that can be defined in a number of different ways. There is no set of neutral, inevitable or objective principles to define what privacy means. Philosophical approaches to the study of privacy have focused on the normative questions around whether privacy is a right, a good in itself, or an instrumental good.[358] Economic approaches to

---

[351] See for example, *Hunter v Southam*, paras 15-16; *Tessling*, para 25; *M(A)*, para 39; *Patrick*, paras 14 and 29.
[352] *M(A),* para 5.
[353] *Hunter v Southam*, para 15.
[354] Hogg, page 36-9.
[355] *Tessling*, para 25. See also Fontana, page 18.
[356] Ronald Krotoszynski, *Privacy Revisited: A Global Perspective on the Right to be Left Alone* (Toronto: Oxford University Press, 2016), page xi. See also Jon Mills, *Privacy the Lost Right* (New York: Oxford University Press, 2008), page 4. See also *Tessling*, para 25, Fontana, page 18.
[357] *Hunter v Southam*, para 25.
[358] James Waldo, et al. *Engaging Privacy and Information Technology in a Digital Age* (Washington: The National Academies Press, 2007) [*Digital Age*], page 1.

privacy have centered around the value, in economic terms, of privacy.[359] Sociological approaches have emphasized the ways in which the collection and use of personal information reflect and reinforce relationships of power.[360] Privacy's inherent uncertainty allows for wide discretion in its application.

Furthermore, not all privacy problems are equal. What is "reasonable" in one situation will not be directly transferrable to another fact scenario. And what is "private" in one context will not necessarily be considered private in another.[361] In assigning meaning to these terms, judges "will inevitably be influenced by their own social, economic and political values."[362] The inherent uncertainty allows for wide discretion in the application of section 8. How the SCC defines "privacy" and "reasonable expectation" are value-laden decisions, ones that greatly impact the protection afforded by section 8 to all Canadians.[363]

The inherent uncertainty of section 8 is evidenced by the regularity of strongly divided judgments.[364] This fracturing shows that Justices at Canada's highest court cannot reach clear conclusions based on the section 8 analysis. In the confusion of split judgments, how are police expected to know the law and anticipate how it will develop in the future with emerging technology?

---

[359] *Digital Age*, page 55. Economics and privacy also consider: consumer valuation of privacy, markets for privacy, the impact of state privacy and data security regulation on companies.
[360] *Digital Age*, page 79.
[361] For example, a file on a personal computer within one's home would attract a reasonable expectation of privacy (see *Vu*), but a similar file on a work computer in a public space attracts a diminished expectation of privacy (see *Cole*).
[362] Hogg, page 36-9.
[363] *Patrick*, paras 14 and 29.
[364] SCC has released split judgments throughout its history on section 8 cases. See for example *Dyment* (1988) split 3:2:1, *Wong* (1990) split 4:2:1, *Kang-Brown* and *M(A)* (2008) both split 4:2:2:1, *Gomboc* (2010) split 4:3:2, *R v Telus Communications Co*., 2013 SCC 16, [2013] 2 SCR 3 [*Telus*] (2013) split 3:2:2, *Fearon* (2014) split 4:3, *Markaha* (2017) split 4:2:1, and *Jones* (2017) split 5:1:1.

4.3.2 Inconsistent Application of the Biographical Core

The vague concepts of "biographical core", "tends to reveal" and "intimate details" leave open a variety of interpretations and there has been confusion in its application.[365] The use of the biographical core as a tool of analysis has been uneven, leading to uncertainty about its exact meaning and its importance in assessing whether section 8 protection is triggered.[366]

The Court of Appeal judgement from *Patrick* is an example of this point. In that case, the accused was suspected of operating an ecstasy lab from his home. On several occasions police took garbage bags that had been placed out for collection but were inside the accused's property line. Based on the evidence found in his garbage, police obtained a search warrant for his house and charged him with unlawfully producing, possessing and trafficking ecstasy. Patrick argued that the police search of his garbage was unreasonable within the meaning of section 8. He was convicted at trial. On appeal, a majority of the Court of Appeal held that the items found in the garbage revealed that the accused "was involved in criminal activity and little else." Therefore, they held the items "cannot constitute intimate details of lifestyle or core biographical details to which privacy protection ought to be extended."[367] The Court of Appeal majority essentially used the biographical core tool as a threshold. In contrast, the dissenting judgement from the Court of Appeal found that "the garbage disclosed information about the appellant's lifestyle and personal choices which led the police to draw conclusions about what the appellant was doing inside his

[365] A biographical core includes intimate details as per *Plant* para 27, but each is a separate component of the analysis as per *Tessling*, para 62 wherein the two are described as two separate considerations.
[366] See "Shriveling of the Biographical Core", at 210 where the authors describe the concept of the biographical core as an "unwieldy concept".
[367] *R v Patrick*, 2007 ABCA 308, [2007] 81 Alta LR (4th) 212 [*Patrick* CA], para 35, see also *Patrick*, para 8.

house."[368] The dissent found a section 8 breach and would have dismissed the charges. This demonstrates uncertainty around defining the biographical core and what is included within it.

Even at the SCC, within one case, there is disagreement on whether to even use the biographical core as part of the section 8 analysis. In 2010, the SCC had the opportunity to use the biographical core analysis in *R v Gomboc* where the utility company cooperated with a police request to install a digital recording ammeter (DRA).[369] Based on the data collected from the DRA, police discovered a pattern of electrical power consistent with a marihuana grow operation and subsequently obtained a search warrant for the residence. Gomboc challenged the search based on section 8 of the *Charter*. The question for the SCC was whether Gomboc had a reasonable expectation of privacy in information about the pattern electricity use disclosed by the DRA. Justice Deschamps, writing for the majority in the result, used the biographical core as a tool of analysis. She looked at the totality of the circumstances including, the nature and quality of the information, its "remoteness from the 'biographical core of personal information" and the legislative scheme in place.[370] She found that this investigative technique revealed the consumption of electricity; nothing about intimate or core personal activities of the occupants.[371] Justice Deschamps explained that:

> Determining the expectation of privacy requires examination of whether disclosure involved biographical core data, revealing intimate and private information for which individuals rightly expect constitutional privacy protection.[372]

As such, she framed the question as a biographical core issue when she went on to write:

---

[368] *Patrick* CA, para 113. See also *Patrick*, para 9.
[369] *Gomboc*, para 1.
[370] *Gomboc*, para 2.
[371] *Gomboc*, at para 14.
[372] *Gomboc*, para 34.

> This brings us to the central issue in this case: whether the DRA discloses intimate details of the lifestyle and personal choices of the individual that form part of the biographical core data protected by the *Charter's* guarantee of informational privacy.[373]

As result of this approach, that there was no foundation for concluding that the disclosure of information revealed any information about household activities of an intimate or private nature; there was nothing that formed part of the biographical core of information deserving of section 8 protection.[374] Justice Deschamps also expressed the view that the DRA revealed "very little about what is taking place in the home".[375] She concluded her reasons on the informational privacy interest with this statement:

> Considerations relevant to the informational privacy analysis therefore lead to the conclusion that no expectation of privacy in the electricity consumption information was objectively reasonable. Disclosing information about electricity consumption is not invasive nor revelatory of the respondent's private life. It does not yield anything meaningful in terms of biographical core data that attracts constitutional protection.[376]

Justice Abella concurred in the result with Justice Deschamps but did so because she found the regulatory scheme determinative. Justice Abella specifically disagreed with Justice Deschamps' conclusion that DRA is not revelatory of activities within the home.[377] Yet she held that Gomboc could not have held a reasonable expectation of privacy in his electric consumption information when the legislation specifically allowed disclosure of customer information to peace officers.[378] Chief Justice McLachlin, writing for herself and Justice Fish, dissenting in the result, disagreed with the majority's restricted understanding of what constitutes a biographical core of

[373] *Gomboc*, para 35.
[374] *Gomboc*, para 36.
[375] *Gomboc*, para 37.
[376] *Gomboc*, para 43.
[377] *Gomboc*, para 81.
[378] *Gomboc*, para 58. See also para 82 where Justice Abella finds that the regulatory scheme "effectively erodes the objective reasonableness of any expectation of privacy in the DRA data".

information. Instead, she took a broader view and reasoned that a search does not have to produce conclusive determinations of activities within a home to be intrusive. She found that by making informed predictions of probable activities in the home, the information conveyed useful private information about an individual's lifestyle which should have attracted a reasonable expectation of privacy and section 8 protection, such that a warrant should have been obtained.[379] In fact, while the biographical core was used by the majority cohort of four in *Gomboc* as a threshold for section 8 informational privacy protection, it was not used by Justice Abella in her concurring judgment for three members of the Court nor the dissent of Chief Justice McLachlin written for two Justices, meaning more Justices of the court did *not* employ biographical core as the threshold for asserting section 8 protection.

As Professor Don Stuart aptly notes in his annotation, the *Gomboc* case reveals "strong divisions and uncertainty on the Court as to how to approach section 8 claims, particularly as to the triggering requirement of a reasonable expectation of privacy."[380] Deschamps' reasoning is reflective of *Tessling*, using the biographical core essentially as a yardstick. However, neither the concurring decision of Justice Abella nor the dissent of Chief Justice McLachlin used the biographical core in their assessments of the case. Therefore, most of the court did not use the biographical core in their reasoning and came to their conclusions through other means. [381]

Within the biographical core tool of analysis, the SCC has created further ambiguity to understanding the scope of the biographical core. In *Plant*, Justice Sopinka approached the biographical core as *including* "intimate details of the lifestyle and personal choices of the

[379] *Gomboc*, paras 124, 132, 137, 141 and 143.
[380] Don Stuart, *Gomboc* case annotation.
[381] For a more in-depth discussion of how the biographical core was used in *Gomboc* in each of the three judgments and a critique of its use, see Stuart Hargreaves, "*R v Gomboc*: Considering the Proper Role of the 'Biographical Core' in a Section 8 Informational Privacy Analysis" (2012) 59 CLQ 87.

individual"[382] whereas in *Tessling*, Justice Binnie presented the biographical core as something different than and distinct from intimate details of lifestyle.[383] In *Gomboc*, Justice Deschamps included intimate details within the "biographical core".[384]

What is included within a biographical core is unknown and confusing. The term "core" suggests that it should include only the central or fundamental aspects. A biographical core would therefore only reasonably include a narrow aspect of one's lifestyle; not be expanded to include personal preferences or likings. For example, if a person is obsessed with tennis – they watch every match, have all the memorabilia and spend their time and money on the sport – that does not form part of their biographical core. In the same way, if a person is a drug dealer and sells illegal substances from their home, that is a part of their lifestyle but cannot be said to raise to the level of becoming a part of their biographical core. As a tool of analysis for determining what should attract section 8 protection, the biographical core ought to be a narrow construction of personal information.

Throughout its irregular consideration, the SCC has sometimes included criminality as part of the biographical core analysis. In *Wong*, Justice LaForest for the majority held that the question whether a person has a reasonable expectation of privacy "cannot be made to depend on whether or not those persons were engaged in illegal activities." He rejected the use of ex post facto reasoning and subsequent validation for searches.[385] Criminality was placed outside consideration

[382] See *Plant*, para 27.
[383] *Tessling*, see paras 32 and 62.
[384] See *Gomboc*, para 36: "The evidence available on the record offers no foundation for concluding that the information disclosed by Enmax yielded any useful information at all about household activities of an intimate or private nature that form part of the inhabitants' biographical core data".
[385] *Wong*, para 19.

as a piece irrelevant to the analysis. However, Justice Lamer, in separate reasons, took a different view as to where criminality fits into the analysis. He explained:

> I agree that such surveillance will violate s. 8 where the target of the surveillance has a reasonable expectation of privacy. However, in my view, the consideration of whether an individual has a reasonable expectation of privacy can only be decided within the particular factual context of the surveillance, not by reference to a general notion of privacy in a free and democratic society which an individual enjoys at all times… Whether such an expectation is reasonable will depend on the particular circumstances; a person does not necessarily enjoy this right in *all* circumstances. It is sufficient to decide this case by considering whether the appellant had a reasonable expectation of privacy in this hotel room which had been effectively converted into a public gaming-house.[386] [emphasis added]

Justice Lamer was including the fact of criminality into his consideration as part of the circumstances.

When *Plant* created the biographical core as a tool of analysis, the majority did not consider the computerized electricity records to reveal a biographical core of information, even though they provided police with information about illegal activities discovered upon the search (a marihuana grow operation). However, in separate reasons, Chief Justice McLachlin expressly included criminality as part of the lifestyle of the accused: "The very reason the police wanted these records was to learn about the appellant's personal lifestyle, i.e. the fact that he was growing marihuana."[387] Since *Plant*, other decisions have taken the view that criminal activity is part of the lifestyle of an accused person; expanding the biographical core and thus what will be protected under the principle of informational privacy. Like Chief Justice McLachlin in *Plant*, in *Kang-Brown* Justice Deschamps expressed:

> The right to informational privacy protects biographical information, including the very nature of the information. In a case involving this right, the relevant elements

[386] *Wong*, para 47.
[387] *Plant*, para 49.

> of informational privacy include intimate personal details about an accused, such as his or her having come into contact with a controlled substance either as a drug trafficker, an illegal drug user or a legal drug user (such as a user of marijuana for medicinal purposes), or by being in the company of drug users. The very personal nature of this information suggests that the appellant had an objectively reasonable expectation of privacy.[388] [emphasis added]

This approach treats drug use or trafficking as part of one's biographical core. Justice Bastarache also treated the information about the contents of the appellant's bag as "within this biographical core".[389]

The SCC marked a shift away from consideration of the biographical core in its reasoning in *Spencer*. The biographical core was mentioned in the *Spencer* decision but only in passing and was not engaged by the SCC in its section 8 analysis.[390] The only time a biographical core of information was even mentioned in argument in the most recent case of *Mills* was in passing by the intervener, Attorney General of British Columbia.[391] Clearly the parties did not think it was worth employing this tool of analysis. As Professors Hunt and Rankin point out, this lack of engagement by both the Court and the parties "serves to minimize the concept's overall importance in the section 8 analysis".[392]

Then in 2017, the SCC was asked whether the sender of text messages, accessed through the recipient's device, has section 8 protection over such messages. In that case, *Marakah*, Chief Justice McLachlin, now for the majority, returned to *Plant* and asserted: "The purpose of s. 8 is

---

[388] *Kang-Brown*, para 175. Justice Deschamps makes the same comments in *M(A)* at para 122: "the odours from A.M.'s backpack might disclose intimate personal details about him, naming his having recently come into contact with a controlled substance either as a drug trafficker, an illegal drug user or a legal drug user (such as a user of medicinal marijuana), or by being in the company of drug users".
[389] *Kang-Brown*, para 227. See also *M(A)* para 157.
[390] See "Shriveling of the Biographical Core".
[391] *Supreme Court of Canada Webcast* for File 37518, online: https://www.scc-csc.ca/case-dossier/info/webcastview-webdiffusionvue-eng.aspx?cas=37518&id=2018/2018-05-25--37518&date=2018-05-25&audio=n, [*Mills* Webcast] at 2:28:12.
[392] "Shriveling of the Biographical Core", 196, 210.

'to protect a biographical core of personal information".[393] She fully accepted criminality as part of the consideration of lifestyle for the biographical core analysis. She explained that:

> The medium of text messaging broadcasts a wealth of personal information capable of revealing personal and core biological information.[394]

And held:

> The mere fact of the electronic conversation between the two men tended to reveal personal information about Mr. Marakah's lifestyle; namely, that he was engaged in a criminal enterprise.[395]

Ultimately the evidence was excluded after holding that Marakah has standing to challenge the search of an electronic conversation between him and the co-conspirator. Clearly the SCC includes criminality as part of the biographical core.

The biographical core has an uncertain place in the section 8 analysis. It has never been precisely defined. It has been unclear from its conception in *Plant*. As it is today, the biographical core analysis will not help the SCC going forward with respect to emerging technologies because the concept is unstable and the information at issue too diverse. Unless the biographical core is clearly defined or expressly rejected as a tool of analysis, lower courts, police, crown, and all justice system participants will suffer.

4.3.3 Case-by-Case Approach and Caveats

The purpose of section 8 is to prevent unjustified state intrusions before they happen.[396] This preventative purpose is disregarded by the SCC when they provide for caveats and adopt a

---

[393] *Marakah*, para 31.
[394] *Marakah*, para 33.
[395] *Marakah*, para 54. See also para 67: "That electronic conversation revealed private information that went to Mr. Marakah's biographical core".
[396] *Hunter v Southam*, para 27.

case-by-case approach. As an example, in *M(A)* Justice Binnie provided a qualification to sniffer dog searches when he said:

> If the lawfulness of a search is challenged, the outcome may depend on evidence before the court in each case about the individual dog and its established reliability.[397] [emphasis added]

The stipulation that the evidence in each case may determine the lawfulness of the search is not wrong. But without more direction, it leaves the search area inexact. Similarly, Justice Moldaver in *Telus* stated:

> I would not go so far as to conclude that a general warrant can never prospectively authorize the delivery of future private communications to the police on a continual basis over a substantial period of time.[398] [emphasis added]

He did not go on to say when this may be possible in some scenario and it is unclear why he would leave such a caveat in that case. Leaving this type of statement in the judgment removes the certainty of the statement that a general warrant cannot authorize prospective production of future text messages. Law enforcement are left thinking they may have that case where a general warrant may apply since it was not decisively removed as an option. Again in *Vu*, Justice Cromwell apparently did not want to make a conclusive statement about computer searches. He explained:

> It is not my intention to create a regime that applies to all computers or cellular telephones that police come across in their investigations, regardless of context. As the respondent correctly points out, police may discover computers in a range of situations and it will not always be appropriate to require specific, prior judicial authorization before they can search those devices.[399] [emphasis added]

This statement provides that police do not always need preauthorization before searching computers or cell phones. Justice Cromwell could easily have stated that the police do require preauthorization unless there are certain conditions or situations. Instead he left a caveat and did

[397] *M(A)*, para 88.
[398] *Telus*, para 107.
[399] *Vu*, para 63.

not provide a "regime". In *Fearon*, Justice Cromwell for the majority again did not take the opportunity to establish a clear rule and instead wrote: "I do not suggest that these measures represent the only way to make searches of cell phones incident to arrest constitutionally compliant".[400] More recently in *Marakah*, Justice McLachlin for the majority dealt with whether the sender of a text message held a reasonable expectation of privacy in the sent text messages on the recipient's device. She held that there was such an expectation of privacy but left a caveat:

> The conclusion that a text message conversation *can*, in some circumstances, attract a reasonable expectation of privacy does not lead inexorably to the conclusion that an exchange of electronic messages *will always* attract a reasonable expectation of privacy … whether a reasonable expectation of privacy in such a conversation is present in any particular case must be assessed on those facts by the trial judge.[401] [emphasis in original]

Further in her reasons, she again provided:

> I conclude that in this case, Mr. Marakah had standing under s. 8 of the *Charter*. This is not to say, however, that every communication occurring through an electronic medium will attract a reasonable expectation of privacy and hence grant an accused standing to make arguments regarding s. 8 protection. This case does not concern, for example, messages posted on social media, conversations occurring in crowded Internet chat rooms, or comments posted on online message boards. On the facts of this case, Mr. Marakah had a reasonable expectation of privacy in the electronic conversation accessed through Mr. Winchester's device; different facts may well lead to a different result.[402]

The continual allowance for caveats leaves an absence of bright lines for police to respect. The Court cannot practically expect law enforcement to be able to prevent unjustified searches before they happen without clarity in the law. Leaving section 8 search issues to be deciphered on a case-by-case basis without clear guidance from the Court creates foreseeable problems, which will ultimately come back to the courts. Litigants will continue to argue opposing yet rational

[400] *Fearon*, para 84.
[401] *Marakah*, para 5.
[402] *Marakah*, para 55.

views. In fact, in some cases the Court actually finds a breach of section 8 but allows the evidence to be admissible because of the uncertainty in the law.[403]

4.3.4 Split Decisions leave Confusion

The seemingly straightforward statement provided in section 8 of the *Charter* has proven to be highly contested. Justices at the SCC are often divided in their reasons[404] and litigants are regularly joined by interveners[405] expressing disagreement on the issues. It seems as though developing technology has added to the confusion.[406]

Split decisions reveal continuing strong divisions and uncertainty on the SCC as to how to approach section 8 cases. Split judgements have made the "majority" hard to find.[407] For example, in *Gomboc* there were three sets of reasons: 1. Justice Deschamps writing for herself, Charron, Rothstein, and Cromwell; 2. Justice Abella writing for herself, Binnie and LeBel, concurring in the result with Justice Deschamps; and, 3. Chief Justice McLachlin for herself and Fish, in dissent. The split was 4-3-2. Within this case, there was a 7-2 split on the result to allow the appeal and restore the convictions. Justice Deschamps and Justice Abella's reasons arrived at the same conclusion – that police can get DRA records without a warrant – but by different routes. However, a different split is found when considering the use of the biographical core. Justice

[403] See *Cole*, *Vu* and *Fearon*.
[404] SCC has released split judgments throughout its history on section 8 cases. See for example *Dyment* (1988) split 3:2:1, *Wong* (1990) split 4:2:1, *Kang-Brown* and *M(A)* (2008) both split 4:2:2:1, *Gomboc* (2010) split 4:3:2, *Telus* (2013) split 3:2:2, *Fearon* (2014) split 4:3, *Markaha* (2017) split 4:2:1, and *Jones* (2017) split 5:1:1.
[405] See for example *Spencer* SCC (2014) with 6 interveners, *Fearon* (2014) with 9 interveners, *Marakah* (2017) with 7 interveners, *Jones* (2017) with 6 interveners and *Mills* (2018) with 9 interveners.
[406] See for example *Telus* (2013) dealing with text messages, split 3:2:2, *Fearon* (2014) dealing with search of a cell phone incident to arrest, split 4:3, *Marakah* (2017) dealing with sent text messages, split 4:2:1 and *Jones* (2017) dealing with a production order for past text messages, split 5:1:1.
[407] When I say a "split" judgment, I am referring to a case where the dissenting Justices are equal in number or more than the majority judgment. For example, with a split of 4:2:2:1 or 4:3:2 it is unclear whether the majority would be a combination of the dissenting judgments, if they all agree on certain points. The majority is not necessarily the largest cohort of Justices on the issues.

Deschamps used the biographical core as a yardstick and her reasons are considered the "majority" judgement. Yet, it was not used by Justice Abella in her concurring judgment for three members of the SCC nor the dissent of Chief Justice McLachlin written for herself and Justice Fish; meaning a majority of the court did not employ biographical core as the threshold for asserting section 8 protection, thus leaving the impression that the biographical core is of limited use to a section 8 analysis for informational privacy. This 5-4 split on use of the biographical core creates confusion.

In the sniffer dog search cases of *M(A)* and *Kang-Brown*, the SCC released fragmented judgements with four separate sets of reasons in each case (the split was 4:2:2:1 in both). In *Kang-Brown*, Justice Binnie recognized that the cases had "polarized" the court.[408] Split judgements reflect indecisiveness from the SCC. The lack of clarity from Canada's top court offers no clear direction to law enforcement. The goal of *preventing* unjustified searches requires clarity in the law for both law enforcement and counsel. Continuing strong divisions from the SCC on how to approach section 8 claims make it difficult for advisory crown and defense to advise their clients and for Canadians to know the limits of law enforcement. If defense counsel and crown counsel do not have clear direction, the result is more litigation and less resolution of cases for courts that are already overburdened.

It is difficult to follow section 8 case law development and predict the outcome on an issue when there is such a lack of certainty. This makes it a challenge to prevent breaches when one cannot foresee how a judgment will split and where the majority will fall. When police are left with lengthy split judgments, it is difficult to understand exactly what the law is. How is the Court going to handle new technology coming when they cannot even agree on how to treat utility

[408] *Kang-Brown*, at para 19.

records?[409] With emerging IoTs and new technologies, these problems will only become exacerbated. They may get worse before they get better if the SCC does not recognize their own inconsistency in approaches to technological section 8 cases. Other than forcing the Court to release only one set of reasons, the solution is likely an overhaul of our understanding of section 8 privacy law as outlined in chapter 5.

4.4 RELEVANT LEGISLATION IS OUT OF DATE

A discussion of search and seizure law is not complete without discussing the relevant legislation. Much of the applicable legislation is outdated and must be contorted to apply to technology that did not exist when it was drafted. At the time Part VI of the *Criminal Code* and search warrant provisions were created, no one was thinking of the upcoming IoTs. Technology develops at a pace which makes it effectively impossible for legislation to keep up. Many times, courts must apply definitions from the *Criminal Code* and make them fit circumstances that were not envisioned by the legislative drafters. For example, section 342.1(2) defines "computer system" as "a device that, or group of interconnected or related devices one or more of which, (a) contains computer programs or other computer data, and (b) by means of computer programs, (i) performs logic and control, and (ii) may perform any other function".[410] This definition does not need amending in order to apply to gadgets that make up the IoTs. Smart home appliances would meet that definition without any need for mental gymnastics. In contrast, section 183 of the *Criminal Code* defines "private communication" as:

---

[409] See *Gomboc*, 2010 (split 4:3:2).

[410] Note this definition of "computer system" dates back to the *Criminal Law Amendment Act*, RSC 1985, c. 27 (1st Supp) with only minor changes since that time. In 1985 the definition of "computer system" read: "a device that, or a group of interconnected or related devices one or more of which, (a) contains computer programs or other data, and (b) pursuant to computer programs, (i) performs logic and control, and (ii) may perform any other function."

> 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. [emphasis added]

This definition includes both an intention and human element. When someone interacts with technology, can that gadget be considered a person or to have intention? For example, can your conversation with Alexa or Siri fit within the definition of "private communication" so as to attract Part VI protections against interception and section 8 *Charter* protection. If the answer is no, can police listen in on people talking to their technology? Based on the definition alone it seems possible, yet the SCC's generous approach to informational privacy suggests they would find a reasonable expectation of privacy in such devices. We have seen the SCC's reaction where legislation does not fit the technology precisely in *Telus*. There the Court dealt with Part VI interception legislation. The majority in *Telus* effectively expanded the definition of intercept of private communications to adapt to technological development of text messages.[411]

If police seized records from an Alexa device, how would the SCC frame the subject matter? It would certainly depend on whether Alexa would be considered a person for purpose of "private communication". The subject matter could be a private conversation in the person's home or a person's one-way verbal commands to technology. What about when the issue deals with smart appliances, such as our coffee pots and fridge. Do police require a search warrant or production order or would they require a Part VI authorization if these gadgets use voice command? Where would wearable technology fit in? FitBits and smartwatches do not clearly fit

[411] Justice Abella, writing for herself and Justices LeBel and Fish, found it was an interception and Justice Moldaver, writing for himself and Justice Karakatsanis, found it was substantially equivalent.

the definition of "private communication" but the information available through that technology is highly revealing.

4.5 THE *MILLS* HEARING AS A DEMONSTRATION OF THE CHALLENGES

The most recent section 8 case to be heard at the SCC is that of *Mills*. It demonstrates the confusion at the SCC when trying to apply section 8 to an online child luring fact scenario. In *Mills*, a police officer created a fictitious Facebook profile appearing as a 14-year-old girl. Over the course of two months Mills, a 31-year old man, communicated with this undercover officer through thousands of messages which were captured by an online tool called Snag-It.[412] The trial judge had found that the police should have obtained prior judicial authorization through Part VI of the *Criminal Code* before seizing the messages.[413] He went on to find that the evidence was obtained contrary to section 8 of the *Charter* but did not exclude the evidence under section 24(2). Mills was convicted of online child luring. The Newfoundland and Labrador Court of Appeal found that Part VI of the *Criminal Code* did not apply and determined that Mills did not have a reasonable expectation of privacy in the messages. The SCC was asked whether Mills had a reasonable expectation of privacy in the communications such that their seizure was a breach of section 8 of the *Charter*. One would think this should be a relatively easy question to answer given the Court's voluminous case law and experience on the subject. Yet when one watches the hearing before our highest court, one is left with the distinct impression that no one really knows what is

[412] Factum of HMTQ, paras 13, 24 and 25.
[413] Factum of Appellant, para 24.

going on. It is not just that there is disagreement on the result or conclusion of the case, there is confusion surrounding how to frame the issue and from which viewpoint to start the discussion.

There were 9 interveners to the case at the SCC.[414] Counsel for Mills started the hearing with the statement that the Mills case was the "first opportunity for this court to be able to develop a principled, purposive, workable approach to covert, proactive, online investigations" … "with some clear guidance to police investigations so that counsel, police and judges will know clearly what the rules are".[415] Counsel went on to argue that the appellant maintained a reasonable expectation of privacy in the communications and suggested that Part VI of the *Criminal Code* was the answer to the section 8 breach. The second counsel for Mills began his comments with the statement "we're on the beginning of a new frontier" … "people's privacy is under siege".[416] Justice Abella responded,

> But isn't social media, can't we look at social media as the voluntary donation of privacy to a public space? … before we say, I believe we have to make distinctions, don't we have to make distinctions between the various kinds of technological places from which we draw this information and I'd be hard pressed to think social media as being privacy protected, it should be, but it isn't… How can we conclude they have even a subjective reasonable expectation of privacy?[417]

The confusion surrounding whether there is any expectation of privacy continued throughout the hearing. Almost all of the Justices had questions about the reasonable expectation of privacy. Justice Brown said "I'm struggling to understand how that could possibly be the subject of a reasonable expectation of privacy".[418] Justice Abella asked whether one party to a conversation

[414] Director of Public Prosecutions, Attorney General of Ontario, Director of criminal and penal prosecutions of Quebec, Attorney General of British Columbia, Attorney General of Alberta, Sumuelson-Glushko Canadian Internet Policy and Public Interest Clinic, Canadian Civil Liberties Association, Criminal Lawyers' Association and Canadian Association of Chiefs of Police.
[415] *Mills* Webcast, at 2:40.
[416] *Mills* Webcast, at 56:00.
[417] *Mills* Webcast, at 1:03:50.
[418] *Mills* Webcast, at 11:00.

can have a reasonable expectation of privacy but the other person does not.[419] Justice Moldaver questioned how an investigation for child luring would ever get started if the police required a Part VI authorization and referenced the need for legislation.[420] Justice Karakatsanis asked whether there could be a reasonable expectation of privacy in a discussion with an undercover police officer and whether the officer could testify as to the conversation.[421] The fact that very basic questions are being asked on section 8 law by the Justices of the SCC is concerning. It seems as though there is more uncertainty than one would expect for an area of the law with over 30 years of jurisprudence.

The Crown's position was that there should be no reasonable expectation of privacy in communications that constitute a crime against the recipient.[422] The problem with that approach, as identified by Justice Karakatsanis and Justice Brown is that is an *ex post facto* determination.[423] However, Justice Moldaver said the obvious answer is that there could be no reasonable expectation of privacy in this situation.[424] Even the basic question of whether there was a search or seizure was debated.[425] Each of the Crown interveners argued that there was no reasonable expectation of privacy and therefore section 8 was not engaged.

There was an obvious and complete lack of agreement on the foundational points between the parties throughout the case at the SCC. The Justices engaged with the parties with questions and discussion throughout the hearing indicating their lack of clarity on the issues. I think there is so much confusion because of the three points identified above – conceptual incompatibility

[419] *Mills* Webcast, 18:20 and 1:42:20.
[420] *Mills* Webcast, at 37:15.
[421] *Mills* Webcast, at 1:18:00.
[422] *Mills* Webcast, at 1:54:40.
[423] *Mills* Webcast, 1:32:25, 1:40:20 and 1:58:50.
[424] *Mills* Webcast, 2:07:35.
[425] *Mills* Webcast, at 2:47:30.

between the normative approach and the analytical tools employed, uncertainty prevalent in the jurisprudence and outdated legislation.

Because of the conceptual disconnect between the intended normative approach and the positive tools of analysis, the parties and the Justices were not able to engage in discussion of the essential values and purpose of section 8. They instead discussed control over the messages and the fact that it was a stranger relationship. The only time the biographical core was mentioned in the hearing was in passing by the intervener, Attorney General of British Columbia.[426] If there was clarity on when and how to use the biographical core as an analytical tool for section 8 cases, the parties could have relied on it. Part VI of the *Criminal Code* was arguably the answer for the case, but because the legislation is out of date with the technology of Facebook and SnagIt, even that was disputed. The trial judge decided that an authorization to intercept private communications under Part VI should have been obtained before seizing the messages. The Newfoundland and Labrador Court of Appeal disagreed. How the SCC will address the legislation's applicability remains unknown, with judgment expected in the Fall of 2018. *Mills* reflects the current state of section 8 law and it is not a pretty picture.

4.6 CONCLUSION

Section 8 jurisprudence suffers from three main disfunctions. There is a conceptual disconnect in how the SCC has approached the normative analysis with positive analytical tools. The cases of *Spencer* and *Marakah* were used to detail how the use of the positive tools (biographical core and totality of the circumstances test) do not match the concerns that genuinely

[426] *Mills*, Webcast, 2:28:12.

motivate them (normative analysis). This incongruity makes it difficult to know how the Court will apply section 8 principles to the next case. In addition to this foundational problem, further uncertainty is apparent. Uncertainty is inherent in the imprecise language of section 8. It is hard to define the boundaries of privacy when such subjective terms are used. There has been an inconsistent application of the biographical core, having its inexact meaning inconsistently applied. The Court's willingness to resort to caveats, use an ad hoc approach and render split decisions compounds the uncertainties within section 8 law. Lastly, outdated legislation is forced to apply to situations that it did not foresee, causing further uncertainty and confusion.

Of course, one needs to recognize the practical limitations of the SCC. They are a reactive body. As an appellate court, they do not have the experts or evidence they may want or need. In addition, the nature of the appellate process does not fit well with rapidly changing technology. Technology at issue in an investigation that comes before the SCC is likely outdated by the time the case reaches its conclusion.[427] The current state of section 8 law is difficult to implement and risks future *Charter* violations. The resulting police uncertainty does not help in the effort to *prevent* privacy breaches.

Considering the challenges identified with the current section 8 jurisprudence, it is not surprising that there is no authoritative answer on how to draw the line between lawful and unlawful searches of technology in criminal investigations. The SCC has been trying to contort the positive analytical tools for section 8 into a normative analysis. They are also trying to apply

[427] For example, the most recent section 8 case dealing with technology to be heard at the SCC was *Mills*. The SCC hearing was May 25, 2018 but the facts arising were from March 2012, that is a 6-year gap between the technology at issue and the SCC's reaction to the case. The judgement is not expected until the Fall of 2018.

that problematic section 8 jurisprudence to current technologies. The next chapter will suggest how the law should be modified to bring greater legal certainty.

CHAPTER 5: MAKING SENSE OF SECTION 8 FOR SEARCHES OF NEW TECHNOLOGIES

5.1 INTRODUCTION

This chapter recommends a way forward for the SCC to better address searches of technology within section 8 parameters. I outline four possible options open to the Court. Each one is meant to minimize the confusion within section 8 jurisprudence. The first option is to continue on the current course of action with no change. The problems identified in chapter 4 would be ignored and the Court would continue conducting business as usual. The second option is to revisit the risk analysis approach. There are benefits to the risk analysis, such as certainty and predictability to be considered. For the third option, I outline a spectrum of privacy protection for the Court to consider employing in section 8 cases dealing with technology. I propose three categories for technology based upon four criteria: intrusiveness, specificity, accuracy and the type of detail involved in the search. The first three of these four criteria are adapted from the SCC's sniffer dog cases, *Kang-Brown* and *M(A)*. As will be explained, the fourth criteria adds the element necessary to deal with technology. Each proposed category of technology would have specialized processes and requirements for searches requiring different levels of prior judicial authorization. These categories could prove to be useful with emerging technologies and benefit from predictability.

The last option I outline for consideration is a move beyond privacy for section 8 protection. Instead of only privacy, the Court could shift the dominant discourse to that of dignity, measuring any infringements with a normative lens. Dignity is a concept not unknown to the SCC's *Charter* jurisprudence and does come with its own challenges. Section 5.5.2 will explore how dignity can be used to develop the Court's approach to section 8 cases. This proposed new framework for the analysis of section 8 cases includes expanding section 8 *Charter* protection in

an understandable and authentic way. It would provide clarity and certainty to law enforcement in the context of criminal investigations when they consider whether a search of technology is lawful or unlawful.

Each of these options will now be outlined as I consider and reject options 1 through 3 to argue in favour of a dignity approach to section 8.

5.2 MAINTAIN STATUS QUO

There is always obviously the option for the SCC to keep things the way they currently are and have section 8 jurisprudence develop along without any serious change. Unfortunately, it is likely that keeping things the same will exacerbate the problems identified in this thesis as technology develops. Foreseeable issues include how the Court will address emerging technologies that will inevitably come before the SCC for consideration. As outlined in chapter 2, section 2.7, technology is more commonly being used as a tool for committing criminal acts. Technology applications and online services are promoting anonymity and secrecy as a feature to their products which stifle law enforcement efforts to investigate crimes on the dark web. The concept of a reasonable expectation of privacy is problematic because it employs analytical tools that are inconsistently applied and frames the question in a positive (instead of normative) way. A reasonable expectation of privacy is vague and uncertain as outlined in chapter 4, section 4.3. Maintaining this threshold concept in a world with dynamically changing norms is concerning.

Law enforcement will most certainly want to take advantage of the growing world of the IoTs as part of their criminal investigations. With the current state of section 8 jurisprudence, they are faced with few concrete answers on lawful parameters to such searches. As our highest court,

the SCC has a responsibility to ensure predictability of section 8 in an effort to prevent unjustified searches. That reasonability cannot be fulfilled by maintaining the current situation. While this is an option, it is not a good one and should be rejected in favour of action.

5.3 RECONSIDER RISK ANALYSIS

The Court could reconsider using the risk analysis for section 8 cases. Instead of using a normative and neutral approach, they would be concerned with protecting only actual privacy. The starting point for the risk analysis "is the proposition that the person who divulges any confidence always runs the risk that his interlocutor will betray the confidence".[428] This approach to section 8 benefits from predictability and certainty. It is a positive approach that would look to factual and measurable indicia of privacy. Either one has or does not have privacy protection based on their level of control over the information. There may be some technology for which people have no actual expectation of privacy and, therefore, would not qualify for section 8 protection. Law enforcement would not require any judicial authority to search those things.

The biographical core and the totality of the circumstances could easily be used under a risk analysis approach to section 8. Both analytical tools are positive and factually driven. Details of financial or medical history would be objectively protected as falling within a biographical core, so long as the person did not expose that information to a risk of disclosure to the State. Similarly, ownership, possession and control could inform the totality of the circumstances in an objective sense to assess whether the person put their information at risk. The fact that these analytical tools fit so well within a risk analysis approach should be concerning when they are employed in a

[428] *Duarte*, para 12.

normative framework. The confusion in the application of the biographical core as a tool of analysis and the place of criminality would still need to be addressed. Precise and exact language is critical since part of the problem is the language used by the Court. A clear definition of what the SCC means by the term "biographical core" would be necessary. I would suggest a return to the first framing of the biographical core in *Plant*. The SCC in *Plant* defined the biographical core as including "information which tends to reveal intimate details of the lifestyle and personal choices of the individual." With that starting point, I would add more definition to that language. Under the risk analysis approach, a biographical core should only include intimate details and personal choices that are actually held in confidence. If individuals do not realistically protect their information, it should not be considered part of a protected biographical core.

The risk analysis has been strongly rejected by the SCC on more than one occasion,[429] primary because privacy would be inadequately protected under that approach.[430] Advanced technology is cited as a concern under the risk analysis, since the State may soon be able to record a limitless amount of information about civilians unless people start becoming hermits.[431] The fears of big brother and an always watching state would be realized under a risk analysis approach to section 8. With the growth of technology, there would be a diminished actual expectation of privacy in our information and a restriction of section 8's protection.

Let's assume we are working under the proposed option – risk analysis – in the context of an Alexa search. Reviewing the material from chapter 2 will assist with this determination. Alexa is really a tool of the advertising and commercial industries to effectively direct market products

[429] For example, see *Duarte* and *Wong*, see also *Cole*, para 76; *Wise*, para 86.
[430] *Wong*, para 11.
[431] "Privacy and the Reasonable Paranoid".

to its users. When the voice commands are captured, they are held by Alexa and used by a corporation. The reality of data breaches and security failures would put an Alexa user's data at risk. When one uses such interactive technology, they assume a risk that their information will be recorded and disseminated in a way that is outside of their control. Given the risk that their information could be obtained by the State, it would not attract privacy protection under section 8.

A look at previously decided judgments perhaps better shows the potential impact of this option. In *Spencer*, the SCC was dealing with a case involving one's IP address, as has been explained in detail in chapter 4.[432] The Court held that Spencer had a reasonable expectation of privacy in the information and that the police were not authorized by law to obtain the subscriber information matching the IP address from the ISP, Shaw communications. If we use a risk analysis, the outcome would likely change. It would be easier to conclude that Spencer had no realistic expectation of privacy in the information gathered from Shaw, being the assigned IP address which led to his geographic location. I say this because Spencer was on a computer in a home that was not owned by him, he was connected to the world wide web in a file sharing, open forum with hundreds, if not thousands, of users who could observe his activity. The IP address, held by an ISP, is shared and known by every website he visited.

Spencer, under a risk analysis approach, would be more closely aligned with the American approach. In *United States v Michaud*, a US District Court dealt with a situation almost identical to Spencer's except that the website was accessed through the TOR network.[433] Jay Michaud lived in Vancouver, Washington and was charged with receipt and possession of child pornography. He applied to have the evidence excluded but the court found he had no reasonable expectation of

[432] See section 4.3.3.
[433] *United States v Michaud*, 2016 US Dist 11033, 2016 WL 337263 [*Michaud*].

privacy in his IP address. The Supreme Court of the United States has developed the third-party doctrine which holds that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties" which means the government can obtain information from a third party without a warrant.[434] Courts in the US have held that "an individual has no reasonable expectation of privacy in his or her IP address, thereby eliminating the need for a warrant".[435] In the US "[e]very federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation".[436] That third party approach in Canada would mean that Spencer did not have a reasonable expectation of privacy, there was no search and, therefore, no *Charter* violation.

Marakah is another case where the determination may have changed had it been based on the risk analysis. The actual privacy we have in our sent text messages is hardly considered secure after we hit send. Chief Justice McLachlin for the majority held that Marakah did not lose control of the electronic conversation simply because another possessed it or could access it.[437] Yet, anyone who sends a message through text actually loses control over the conversation (who can see it, have access to it), unless the maintain control over both the sending and receiving device through a RAT or possession.[438] Once he sent the text message to his accomplice's phone, he took the risk that text message conversation would be disclosed to the State. Justice Moldaver's dissent

[434] "The Digital Underworld", at 111.
[435] "The Digital Underworld", at 116; *United States v Ferrell*, 2016 WL 705197 (2016), at 1; *United States v Matish*, 193 F Supp 3d 585, 2016 WL 3545776 (2017), at 20-21; *United States v Werdene*, 188 F Supp 3d 431, 2016 WL 3002376 (2016); *Michaud*, at para 7.
[436] *United States v Perrine*, 518 F3d 1196 (10th Cir 2008); See also: *United States v Bynum*, 604 F3d 161 (4th Cir 2010); and *United States v Stults*, 575 F3d 834 (8th Cir 2009).
[437] *Marakah,* para 41.
[438] Possession could be physical possession of the device, joint possession with another person or constructive possession through means such as intimidation or threat. In each of these cases, the person would exert control over the electronic conversation to maintain privacy protection.

in *Marakah* aligns with this approach to restrict section 8 to realistic expectations of privacy. As he expressed within his dissenting judgment:

> Here, Mr. Marakah had no control whatsoever over the text message conversations on Mr. Winchester's phone. Mr. Winchester had complete autonomy over those conversations. He was free to disclose them to anyone he wished, at any time, and for any purpose. To say that Mr. Marakah had a reasonable expectation of personal privacy in the text message conversations despite his total lack of control over them severs the interconnected relationship between privacy and control that has long formed part of our s. 8 jurisprudence. It is equally at odds with the fundamental principle that individuals can and will share information as they see fit in a free and democratic society.[439] [emphasis added]

Had this been the majority judgment, the expectation of privacy analysis would more closely fit the risk analysis approach. These case examples, of *Spencer* and *Marakah* are used here only to illustrate the point that the SCC would likely come to different conclusions if the risk analysis were the approach applied to section 8 cases.

Adopting the risk analysis would affect how the Mills case is decided. Through communicating on Facebook with a minor, Mills took the risk that the child would betray the confidence. He did not know who was on the other end of the communications. The fact that it was a police officer who was able to testify as to the exchange was a risk he took by engaging in the child luring on the internet.

This risk analysis option would likely be rejected by the SCC without too much consideration because it does not fit well with Canadian values. As Justice Côté put it: "Canadians are not required to become digital recluses in order to maintain some semblance of privacy in their lives."[440] The adamant rejection of the risk analysis would likely continue.

[439] *Marakah*, para 99.
[440] *Jones*, para 45.

5.4 A SPECTRUM OF PRIVACY PROTECTION

In this section outline a third option for the Court to consider – a spectrum of privacy protection for section 8 cases dealing specifically with technology. This proposal is most closely aligned with and builds upon current jurisprudence – different levels of justification and procedural requirements based on the level of privacy implicated. Parliament has recognized, and the legislation reflects, varying degrees of prerequisites for different types of searches based on the type of information collected. Who can authorize and apply for certain search warrants and what offences qualify varies according to the type of search involved. For example, a search warrant pursuant to section 487 of the *Criminal Code* provides that a "justice"[441] may issue a search warrant but an interception for private communications requires a judge[442] of the superior court of the province, unless there is a consent to the interception.[443] Certain warrants require that the authorization be applied for by the Attorney General instead of simply a peace officer.[444] The *Criminal Code* outlines the legal thresholds that law enforcement must establish for obtaining interception of private communications, search warrants, general warrants and production orders. The legal standard for each of these authorizations ranges from "reasonable grounds to believe"[445] to "reasonable grounds to suspect".[446] After certain warrant-specific preconditions have been met,

[441] "Justice" defined in section 2 of the *Criminal Code* means "a justice of the peace or a provincial court judge".
[442] "Judge" defined in section 552 of the *Criminal Code* means "a judge of the superior court of criminal jurisdiction in the Province". See section 185 of the *Criminal Code* for details of the Application for a Part VI Authorization.
[443] See section 184.2 of the *Criminal Code*.
[444] See for example section 185 of the *Criminal Code*, setting out requirements for an application for authorization to intercept private communications, which requires the application made and signed by the Attorney General or the Minister of Public Safety and Emergency Preparedness or an agent specially designated.
[445] See sections 184 for authorization to intercept private communications, 487 for search warrant, 487.01 for general warrant, 487.014 for production order.
[446] See sections 487.015 for production order to trace specified communication, 487.016 for production order – transmission data, 487.017 for production order – tracking data, 487.018 for production order – financial data. Part VI of the *Criminal Code* sets out a comprehensive scheme for the interception of private communications, which requires

police may conduct a search of a specified place in relation to a specified offence. As the degree of intrusiveness increases so too do the conditions attached to obtaining the warrant. For example, in order to obtain an authorization to intercept private communications, one of the more intrusive search tools available to law enforcement, the application must demonstrate investigative necessity.[447] There are recognized exceptions to the requirements of prior judicial authorization such as customs border searches, search incidental to arrest, circumstances of urgency and dog sniffer searches.[448] In this way, the law already recognizes a continuum of constitutionally valid standards for privacy protection.[449] The difference with this option is that the spectrum I propose is explicitly and specifically meant to address informational privacy in emerging technologies.

There are infinite shades of gray regarding online privacy.[450] A spectrum of privacy protection would match this reality. As Justice Binnie noted in *M(A)*, all searches "do not have the same invasive and disruptive quality".[451] This continuum of lawful standards could allow for searches of technology to be clearly and predictably reasonable, without prior judicial authorization in some circumstances. Looking at the "intermediate standard" in *M(A)* for sniffer dog searches is helpful for creating a new standard for emerging technology. In that case, the SCC found that because the search was minimally intrusive, specific in nature and had pinpoint accuracy, a new threshold was needed. The related case of *Kang-Brown* explained that the lower

more than "reasonable grounds to believe"; see s. 185(1)(h) for investigative necessity requirement, see (1.1) for exception for criminal organizations and terrorist groups.

[447] See section 185 of the *Criminal Code*, note there is an exception to this requirement for offences related to criminal organizations and terrorist groups.

[448] Fontana, page 6. See also *Kang-Brown* and *M(A*), the standard of reasonable suspicion for sniffer dogs, border crossings (*Customs Act,* s. 98), corrections context (*Corrections and Conditional Release Act*, SC 1992, c 20, s. 49); areas were lesser expectation of privacy. See also section 184.4 of the *Criminal Code* which allows the warrantless interception of private communications in exigent circumstances to prevent serious harm.

[449] See *Kang-Brown*, para 169.

[450] Lori Ruff, *#Privacy Tweet: Addressing Privacy Concerns in the Day of Social Media* (California: THINKaha, 2010), page 22.

[451] *M(A*), para 13.

standard was "pragmatic and balanced"[452] for sniffer dog searches partly because it was minimally intrusive – the dog did not touch the person, the dog's indication was subdued, the search did not require a significant amount of time or undue inconvenience and did not interfere with bodily integrity.[453] In addition, the SCC considered the specific nature of the search – the only personal information revealed by the search is the presence or absence of drugs. The last consideration was the pinpoint accuracy of the search.[454]

If one transposes these three considerations into the technology context, it becomes clear that much technology would meet the criteria of being minimally intrusive, specific and having pinpoint accuracy. Minimal intrusion occurs when police search technology. In many instances, the person does not even know a search occurred, there is no inconvenience and it does not interfere with bodily integrity. Even though technology searches can engage significant information privacy interests, not every search will be a significant intrusion.[455] Certainly the level of intrusion would depend on the technology at issue. The data collected from a wired coffee pot, fridge or other home appliance would likely not rise to the level of being considered a significant intrusion. As to the specific nature of the search, technological searches can be restricted to only obtain the precise information sought. Lastly, with respect to pinpoint accuracy, with a narrow target and precise search, technology is more accurate than the best sniffer. One should ask if the SCC's intermediate standard is appropriate for certain technology searches. Because of the SCC's continued recognition of a heightened expectation of privacy in computers and cell phones, it is

[452] *Kang-Brown*, para 166.
[453] *Kang-Brown*, para 242.
[454] *Kang-Brown*, paras 234-238.
[455] See *Fearon*, paras 54 and 63.

not likely this particular technology that would fit the new standard. However, the IoTs has yet to be adjudicated by the SCC and leaves room for such consideration.

Where should the IoTs technology fall on a privacy continuum compared to a dog sniff? While sniffer dogs are "incredibly powerful and reliable tools," so too is technology.[456] Allowing for a continuum of protection recognizes that different technological devices may, in fact, fall at different places on that spectrum. Application of this idea to the IoTs requires answering when an authorization is required, who can apply for it and grant it and what, if any, conditions there would be to such authorization. Because not all technology is the same, the answer cannot be uniform for all devices. The use of categories will illustrate how this approach could be applied.

5.4.1 Category #1 – "Smart" Technology that is "Dumb"

Some of our "smart" technologies are relatively "dumb" in the sense that while they are embedded in household goods and connected to the internet or other devices, they cannot listen or respond to their owner. Such devices would include the smart fridge that knows every time the door has opened and stores the time in a database, or the light bulb that detects particular movement. These devices transmit a message wirelessly to a server whenever there is activity.[457] This digital information does not reveal a massive amount of information about the device's user but the specific data it does reveal may be useful to police. For example, if police are trying to find out if someone who lives in a rural area is home at a particular time, the information about their fridge and light bulbs would help. They cannot drive right up to the home to look for themselves so if the data tells them that the fridge door was opened 5 minutes ago, and the lights

[456] *Kang-Brown*, para 220.
[457] *Spy in the Coffee Machine*, pages 14-16.

are on, they can assume someone is home. This is just an assumption based on data, but it is better than a blind assumption.

Any search to obtain data from a dumb device would be minimally intrusive, specific and have pinpoint accuracy.[458] It is minimally intrusive because the search does not require law enforcement to enter the home, does not touch the person or require them to do anything, causes no inconvenience nor interfere with the subject's bodily integrity. It is specific in nature. The only information revealed by the search is data about that particular device. The search is very restricted because no other information would be obtained. The results of the search would be a list of dates and times indicating on or off for the light bulb. Lastly, the search would have pinpoint accuracy. The data is precise and more accurate than any human observation. While the device is in someone's private residence, the search actually takes place at the location of the server where the data is stored.

In addition to the three considerations outlined above and adapted from the sniffer dog cases, in this continuum for technology it is important to have one additional consideration – the type of detail involved in the search. For Category #1 devices, I suggest that the information obtained is mundane. On its own it does not tell much about a person. I would imagine that the SCC would treat this type of technology must like they did the FLIR or DRA. Like FLIR, the information "may or may not be capable of giving rise to an inference about what was actually going on inside"[459] And similar to DRA, the information disclosed is not of an intimate or private nature, not confidential like a doctor-patient relationship nor does it disclose political affiliation,

[458] Note, I have adapted these three considerations from the sniffer dog cases of *M(A)* and *Kang-Brown*.
[459] *Tessling*, para 27.

sexual orientation, etc. of the user.[460] These devices in Category #1 provide a pattern of use of a device.

A discussion of this category would not be complete without addressing Chief Justice McLachlin's concerns raised in *Gomboc*. In that case, she expressed a concern about DRA technology as follows:

> Our consent to these "intrusions" into our privacy, and into our homes, is both necessary and conditional: necessary, because we would otherwise deprive ourselves of services nowadays considered essential; and conditional, because we permit access to our private information for the sole, specific, and limited purpose of receiving those services.[461]

The difference with "smart" devices is that they are totally optional, unlike electricity use in the case of DRA data. Smart devices are not "essential" to our lives. They are likely nice to have as a luxury but certainly not required in order to live a fulsome existence. Not having the newest technology embedded in our homes is currently not unusual. That may, of course, change in the next decade but for now Chief Justice McLachlin's concerns do not apply to the dumb devices in Category #1.

Now that I have outlined what Category #1 would look like, it is essential to outline any prerequisites for searches of these devices. For this category of technology, I suggest that police be permitted to search Category #1 devices on a reasonable suspicion standard without requiring judicial preauthorization. Justice Binnie succinctly explained the reasonable suspicion standard in *Kang-Brown*:

> The "reasonable suspicion" standard is not a new juridical standard called into existence for the purposes of this case. "Suspicion" is an expectation that the

[460] See *Gomboc*, para 7.
[461] *Gomboc*, para 100.

> targeted individual is possibly engaged in some criminal activity. A "reasonable" suspicion means something more than a mere suspicion and something less than a belief based upon reasonable and probable grounds.[462]

A reasonable suspicion is not speculation but rather is objectively verifiable evidence that a crime will be or has been committed. Where a reasonable suspicion exists, a search of Category #1 devices would be authorized by the common law as it was in *Kang-Brown*,[463] given the minimally intrusive nature of the search, specific target and pinpoint accuracy of the search through technology. A search would still fail to be reasonable if there is an absence of reasonable suspicion or if the search is not conducted reasonably. These safeguards of the reasonable suspicion standard and a reasonable search prevent police from randomly spying on people or spying based on a hunch.

While there are judicial pre-authorizations on a suspicion standard within the *Criminal Code* for certain production orders[464], I propose that no judicial authorization would be required for Category #1 for efficiency and practical reasons. Police will likely want to engage Category #1 devices frequently. The implications of requiring already overburdened courts to deal with applications for searches of Category #1 devices are obvious – investigative delays and more paperwork for judges. Realistically, if police are contemplating searching a Category #1 device, they will also likely be seeking to search devices under Category #2 and/or Category #3, which do require judicial authorization. I would not want to add more responsibility to the courts when this category engages such relatively minor privacy interests.

---

[462] *Kang-Brown*, para 75.
[463] See para 60.
[464] See for example section 487.015, Production Order to trace specified communication; section 487.016, Production Order for transmission data; section 487.017, Production Order for tracking data; section 487.018, Production Order for financial data.

5.4.2 Category #2 – Technology that Potentially Reveals Sensitive Information

I propose that the devices in this category are more than sensors and are capable of ascertaining sensitive information about the user's lifestyle. These would include devices such as a smart watch, Fitbit, or other wearable technology and devices that capture personal information. While wearable technology likely all have GPS capability and can therefore be used for tracking a person, I am only concerned with the search of all data from these devices, not just the tracking function specifically.[465] Smart watch devices and smart beds record and store information about the user's heart rate and sleep patterns.[466] This medical-like information is higher on the spectrum of privacy than whether a light bulb is on or off.

Searches of the devices in this category are still minimally intrusive, specific in nature and have pinpoint accuracy. Similar to Category #1, law enforcement does not enter the home, touch the person or require them to do anything, cause inconvenience or interfere with bodily integrity. Again, the information revealed by the search is the specific data about the device and it is exact. However, the difference comes with the added consideration of the type of detail discovered. For Category #2 devices, the information cannot be described as mundane because it can reveal a pattern of use of an individual user and details about their lifestyle. While the biographical core analysis could be used here, it is not necessary to understand the point that this technology, in

[465] Note, to use these devices as a tracker, section 492.1(2) would be engaged, which requires reasonable grounds to believe that an offence has been or will be committed and that the tracking will assist in the investigation of the offence.

[466] See Wareable, "Best Heart Rate Monitors: Top Watches, Chest Straps and Fitness Trackers" online: https://www.wareable.com/fitness-trackers/best-heart-rate-monitor-and-watches. For beds, see Sleep Number, "Explore the Sleep Number 360 Smart Bed" online: https://www.sleepnumber.com/360. The website advertises that the bed "knows how you're sleeping" with SleepIQ technology inside the bed to track how well you sleep each night.

Category #2 provides the type of detail deserving of some protection higher on the spectrum than those in Category #1.

For law enforcement to legally search the devices in Category #2, I suggest that police proceed on a reasonable grounds standard and seek judicial pre-authorization. This standard is the one for tracking devices for tracking an individual's movements within the *Criminal Code*[467] and makes sense as we move to more sensitive information. Police would be required to demonstrate on oath reasonable grounds to believe that an offence has been or will be committed to the satisfaction of a judicial officer. I propose, similar to the tracking warrant provision that either a justice or a judge can be the recipient of such applications.[468]

5.4.3 Category #3 – Smart Technology that is (Too) Smart

The devices in Category #3 are truly smart devices. They are devices that we interact with, either through voice commands or programming. These devices can listen and respond to us. Smart televisions with cameras, microphones and speakers and digital assistants such as Alexa would be included in this category. I say these devices are too smart because they have the ability to surreptitiously listen to our daily ramblings and record massive amounts of information about us that we likely would not want shared with anyone. Searches of these devices indisputably and effectively amount to an invasion of privacy and the protections outlined within Part VI of the *Criminal Code* should be the starting point for any search or seizure. Before police are granted access to the data (including voice communications) of such devices, they would need reasonable and probable grounds to believe that an offence has been or will be committed. As for what

[467] *Criminal Code,* section 492.1(2).
[468] The reason I propose emulating the tracking provision found in section 492.1(2) of the *Criminal Code* is because that tracking warrant provides factually similar information – data – as opposed to a section 487 general warrant which is used commonly in physical searches for tangible things (i.e. weapons, drugs, etc.).

offences would qualify, the list of offences provided in section 183 of the *Criminal Code* would seem to make a good starting reference point. The other safeguards set out in Part VI of the *Criminal Code* – limited period of authorization and investigative necessity would be equally applicable. Additional requirements for Category #3 devices should also be considered since the information gathered is actually more than just what was said in an intercepted conversation; it includes data such as where the person was when they were talking, how long they were speaking, who they were talking to, that other person's contact information, the history of their communications, etc. Protections may include mandatory live monitoring, but the judge should be given wide latitude to set out appropriate terms and conditions to the order. If you consider an Alexa's ability to record data, this device is a room probe, video camera and audio recording device. As with Part VI authorizations, only judges of a superior court of criminal jurisdiction should be permitted to authorize such searches given the serious intrusion on privacy.

The ideal solution for voice command devices would be for the definition of private communications within the *Criminal Code* to be expanded to include conversations with devices. Considering the future of technology includes increasingly common Artificial Intelligence devices, this solution would have wide reaching application. The current definition of "private communication" reads:

> 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.[469]

[469] *Criminal Code*, section 183.

Parliament could amend the definition simply as follows:

> 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~~.

In the meantime, the SCC can interpret communications with devices as substantively equivalent to private communications. This would be similar to what Justice Moldaver did in *Telus* when he found that the investigative technique was substantively equivalent to an intercept, as defined in the *Criminal Code*.[470]

As Justice Binnie noted in *Tessling*, the reasonableness of the search has to be determined by looking at current, not potential future, of technology capabilities.[471] A device may transition from Category #1 to Category #2 or even #3. It is not hard to image a fridge soon having a microphone and speaker to accept voice commands. While this creates some uncertainty, knowing each of the categories and what the consequences will be does provide some level of predictability; certainly, more than simply saying any evolution in the future will be dealt with by the courts on a step by step basis as was done in *Tessling*.[472] While I suggest three categories I am sure that the IoTs could make up 10 or more categories. However, the usefulness of more categories did not seem to be useful given the three search thresholds: reasonable suspicion, reasonable belief or reasonable belief plus.

[470] *Telus*, paras 49 and 67.
[471] *Tessling*, paras 29 and 55.
[472] *Ibid*.

This spectrum approach acknowledges that not all technology is the same and does not present the same information nor should it attract the same privacy protection; one cannot use same analysis for a fridge as for Alexa. Given the breadth of gadgets that make up the IoTs, some searches would be minimally intrusive while others would not. This spectrum approach also allows courts to recognize a heightened, reduced or non-existent privacy interest where appropriate.

5.4.4 A Hypothetical Scenario – Mr. Criminal and his Technology

A hypothetical scenario will demonstrate the likely consequences of this proposed spectrum. Mr. Criminal is running a drug trafficking operation from his increasingly common and typical smart home. He owns a smart television that has voice control[473] and a smart fridge.[474] For Christmas last year his parents bought him a Fitbit and an Alexa, both of which he uses every day. Mr. Criminal is a typical Canadian, having a Facebook profile where he shares photos of himself and his family at BBQs and hanging out at home. He communicates with his underlings via text message from his smart phone; telling them when and where to pick up and deliver the drugs.

Police have suspected Mr. Criminal of being involved in drug trafficking. Their suspicions are based on intelligence gathered through multiple credible informants who tell them that Mr. Criminal brings large shipments of cocaine, heroin and Fentanyl into Canada and uses a local network of drug dealers to distribute the drugs throughout the Maritimes. They are also told that

[473] See for example, LG, "LG OLED TV AI ThinQ" online: https://www.lg.com/ca_en/oled-tv/AI.jsp?cmpid=2018HQSEM_TV_CI-EN_Smart-AI-Generic_Exact-0628_Sma_rt-TV_k3598&gclid=CjwKCAjw7IbaBRBqEiwA6AyZguPZAtfmG1Wq-DK2T8Z67onav3_kxYa511LfRWGY4mlKBhdtwBXVTxoC2mAQAvD_BwE#intro.

[474] See for example, LG, "Refrigerators" online: https://www.lg.com/ca_en/refrigerators?cmpid=2018HA-SEM_CI_Google_Refrigerator-1806-EN_Smart_k0149_pc&gclid=CjwKCAjw7IbaBRBqEiwA6AyZgpG57m1N18-6WJeNbf-whsyBtwl_EQas5_xh23HDzxUjlxE2_ywt2xoC8T8QAvD_BwE.

Mr. Criminal is single and lives alone. Police use open source internet searches to canvass Mr. Criminal's social media activity hoping to gather information about his activities as part of their preliminary investigation. No search warrant is needed for gathering this information since it is an open source search, open to everyone on the internet. Mr. Criminal must not have set his privacy settings on his Facebook profile set to "private" because police easily find lots photographs of Mr. Criminal. In some photographs he is out with his friends at local pubs and restaurants. Police can identify those individuals from their experience as known and convicted street level drug dealers. There are also photographs of Mr. Criminal around his home during what appears to a family BBQ. Police use this information to corroborate the details provided by the informants. Police can see the smart television and fridge along with an Alexa machine in the background. Comments on his social media pages also give insight. For example, Mr. Criminal's product review of Alexa confirms he owns that product. His "like" of a Fitbit and related comments also tell other users that he has one, uses it and likes it. Mr. Criminal has an open dating profile where he says he is single and lives alone. Mr. Criminal does not appear to ever attend employment or comment on work in his social media accounts, yet he boasts about having a new home and driving a jaguar.

With the above information from confidential informants being credible, corroborated and current, police have reasonable suspicion to believe that Mr. Criminal is committing the crime of drug trafficking pursuant to section 5 of the *Controlled Drugs and Substances Act*.[475] At this point, they could search devices within Category #1 without a judicial authorization. They decide to

[475] SC 1996, c 19.

search Mr. Criminal's smart fridge by accessing its data to find out the pattern of his activity. They discover that last week he opened the fridge door as follows:

> Monday – 3:34am, 3:40am, 9:38am, 2:52pm, 6:03pm, 9:20pm and 10:59pm
> Tuesday – 3:30am, 3:37am, 9:35am, 3:05pm, 6:10pm, 9:00pm and 10:45pm
> Wednesday – 3:36am, 3:44am, 9:40am, 4:00pm, 6:15pm, 9:12pm and 11:02pm
> Thursday – 3:34am, 3:40am, 9:38am, 1:52pm, 6:03pm, 9:20pm and 10:59pm
> Friday – 3:32am, 3:38am, 9:42am, 2:58pm, 6:03pm, 9:03pm and 11:10pm

Based on the above data, police discovered that Mr. Criminal is awake every weekday around 3:30am. He then appears to be active again by 9:30am. He is home during the day because he opens the fridge door again in the afternoons between 2 and 3pm and in the evening around 9pm. The last time the door is opened every day is 11:10pm indicating he is likely home for the evening. This data leads to an assumption that Mr. Criminal does not work a 9am to 5pm job, since he is home throughout the hours of the day. The activity around 3:30am is somewhat suspicious, but not determinative, and so police decide to focus their energies on the target at that time, thinking perhaps that is when he is conducting illegal activity.

After conducting significant physical surveillance of Mr. Criminal in the early morning hours, police discover Mr. Criminal regularly leaves his residence between 3:45am and 4am to meet with individuals who are known to be involved in the drug trade at an abandoned parking lot. Over the course of several months, police continue their surveillance and discover a pattern of meetings. They decide to conduct traffic stops on vehicles of Mr. Criminal's associates after the two have met. On two occasions they discovered kilograms of cocaine in the vehicles of the associates.

The police decide that they want to purse an investigation into Mr. Criminal. The next investigative steps would involve gathering more digital data. They want to use his Fitbit as a

tracking device, so they can follow him with physical surveillance without getting too close. There are provisions in the *Criminal Code* that allow police to apply to a justice or judge for tracking the location of an individual through a device, which includes a computer program.[476] They must have reasonable grounds to believe that an offence has been or will be committed. In this fact scenario, the police can use Mr. Criminal's Fitbit program to track him. In addition to tracking him, police want to access the other data available through Mr. Criminal's Fitbit to glean information about his sleep patterns and heart rate. This information would provide insight into what he is doing when he is home during the day, i.e. if he sleeps all afternoon this adds to the police theory that he is living off the proceeds of crime instead of working from home. The search for this data still falls within the Category #2 class of devices and would require judicial authorization based on reasonable and probable grounds to believe that an offence has been or will be committed. In addition, police will have to expressly demonstrate what they are looking for in the data and how that will aid in moving their investigation forward.

The results of the search warrant for Mr. Criminal's Fitbit shows that he does in fact sleep most days between 11:00pm and 3:30am and again between 10:00am and 2:00pm. The police are still not able to get close enough to Mr. Criminal or any of his associates to know the details of the drug shipments or where the drugs are coming from. The police want to know who he talks to on a regular basis and confirm whether in fact Mr. Criminal is a high-level drug dealer. They want to learn where he gets the drugs from and to whom he sells them, so they can capture the entire drug ring for prosecution. The police decide they have a plan to gather all that information. They want to obtain access to Mr. Criminal's devices – the smart television and Alexa in his residence. They think if they hack into the technology and activate the microphones, they can listen in on

[476] *Criminal Code*, section 492.1.

everything he says. That would clearly be a private communication within the definition of the *Criminal Code* and an authorization would be needed.[477] Any search conducted of the smart television with audio and video recording abilities or Alexa device would require the Category #3 approach. The police will be required to apply to a judge of the superior court for an authorization. Their application must outline their reasonable and probable grounds to believe that a specified offence has been or will be committed, the time period they seek the interception and how it is necessary to the investigation.

Under this proposed option, the Court would be able to eliminate the confusion surrounding the concept of a reasonable expectation of privacy since there would be no need to consider it. This option – a spectrum of privacy protection – provides the concrete benefits of certainty and predictability that are the cornerstone of section 8. This option is less normative and more positive in its approach but achieves the purpose of section 8 in a practical way. The categories within this spectrum are able to expand as required by technologies that do not yet even exist. Under this approach, the balance between individual privacy and law enforcement would be clearly understood such that judicial actors could be engaged when required by the privacy interest at issue.

5.5 MOVE SECTION 8 BEYOND PRIVACY

Perhaps we have reached full circle. We are back to the comments of Justice Dickson in *Hunter v Southam* when he said:

> Like the Supreme Court of the United States, I would be wary of foreclosing the possibility that the right to be secure against unreasonable search and seizure might

[477] *Criminal Code*, section 183.

> protect interests beyond the right of privacy, but for purposes of the present appeal I am satisfied that its protections go at least that far.[478]

Justice Dickson did not need to consider section 8 beyond privacy in *Hunter v Southam* because it was not necessary for that case. The pervasiveness of technology demands that we consider this option for section 8, beyond the right of individual privacy. What would a future with search and seizure protection beyond privacy look like? How can the line be drawn between lawful and unlawful searches of technology in the context of criminal investigations? Move beyond simply *privacy*. This can be done through 1) a collective understanding of privacy and 2) appreciating a broader understanding of section 8 to address the genuine underlying concern of *dignity*.

5.5.1 Section 8 as a Collective Right

As discussed in chapter 3, section 3.3, the SCC has framed section 8 privacy protection as an individual right. With that premise, the implication of a *Charter* violation under section 8 currently can result in an exclusion of evidence from the trial of an accused pursuant to section 24(2) of the *Charter*. That is an individual specific result. But we are living in a culture with pervasive technology and little actual control over our data. Because technology has connected our devices and ourselves to many other individuals and corporations, breaches of privacy now have a ripple effect on a multiplicity of people. Section 8, viewed as a collective right, recognizes and acknowledges the connectivity of society through technology as discussed in detail in chapter 2. As Justice LaForest noted in *Edwards* back in 1996, section 8 should not be limited as an individual right but rather can be viewed as a collective value recognizing with our shared values of sociality, connectiveness and openness. This assertion of a collective right is explicit in the *Charter*'s recognition that "everyone" is protected from unreasonable searches or seizures.

[478] *Hunter v Southam*, para 25.

When one person's section 8 rights are breached, the impact could be wider ranging than simply an exclusion of evidence for that particular accused person. For example, the Court could extend any exclusion of evidence to related trials or provide stays of proceeding pursuant to sections 8 and 24(1) of the *Charter*. They have this ability currently through Section 7 together with section 24(2) of the *Charter* to exclude evidence or order a stay of proceedings as a matter of trial fairness.[479] However, on a collective understanding of section 8 the Court would not need to resort to the residual protection of section 7. If evidence was obtained by an unconstitutional search or seizure, such that it was excluded for the accomplice, it would not be fair to be able to use the text messages against the other party to the conversation. The Court can appreciate that in today's technology world, we are connected to a larger degree than ever before and our rights are not as exclusive as they once were.

This approach is within the jurisdiction of the judiciary and strengthens the Court's protection of privacy in our digital age. Currently the section 8 analysis is to balance competing values; *individual* interests and rights against our *collective* preference and desire for security. It seems a fairer contest would be if the balancing were instead a *collective* right against *collective* security. Perhaps then the scales would balance differently.

5.5.2 Dignity as a Primary Concern

The place of dignity within current section 8 jurisprudence was detailed in chapter 4, section 4.2.3. There I argued that the core concern underlying all search and seizures cases is really dignity. The goal of section 8 of the *Charter* is to prevent searches and seizures that present an affront to human dignity. That is what search and seizure does, it intrudes on our dignity. If

[479] *R v Jewitt*, [1985] 2 SCR 128, 21 CCC (3d) 7. See also *Marakah*, para 192.

the State does not have proper lawful authorization, that search is unreasonable and therefore unlawful.

Without more, using the concept of dignity brings no more clarity to section 8 jurisprudence. The Court must explain what they mean by dignity in the section 8 context and explain how a framework of dignity will protect against *Charter* violations. This can be done by drawing on the Court's wealth of jurisprudence in other *Charter* cases. As Justice Wilson commented, the "*Charter* and the right to individual liberty guaranteed under it are inextricably tied to the concept of human dignity".[480] Dignity is an underlying value that "finds expression in almost every right and freedom guaranteed in the *Charter*".[481] This idea is also found in Chief Justice Dickson's (as he then was), discussion of *Charter* interpretation in *R v Oakes*,

> A second contextual element of interpretation of s. 1 is provided by the words "free and democratic society". Inclusion of these words as the final standard of justification for limits on rights and freedoms refers the Court to the very purpose for which the *Charter* was originally entrenched in the Constitution: Canadian society is to be free and democratic. The Court must be guided by the values and principles essential to a free and democratic society which I believe embody, to name but a few, respect for the inherent dignity of the human person, commitment to social justice and equality, accommodation of a wide variety of beliefs, respect for cultural and group identity, and faith in social and political institutions which enhance the participation of individuals and groups in society. The underlying values and principles of a free and democratic society are the genesis of the rights and freedoms guaranteed by the *Charter* and the ultimate standard against which a limit on a right or freedom must be shown, despite its effect, to be reasonable and demonstrably justified.[482]

Section 7 of the *Charter* can inform section 8 jurisprudence.[483] In the *per curiam* judgment of *Carter v Canada*, the SCC struck down the *Criminal Code* prohibition of assisted suicide

[480] *R v Morgentaler*, [1988] 1 SCR 30, 37 CCC (3d) 449 [*Morgentaler*], para 285.
[481] *Morgentaler*, para 288.
[482] *R v Oakes*, [1986] 1 SCR 103, 24 CCC (3d) 321, para 67.
[483] Hamish Stewart, *Fundamental Justice: Section 7 of the Canadian Charter of Rights and Freedoms* (Toronto: Irwin Law Inc, 2012) at page 6. See also *R v O'Connor*, [1995] 4 SCR 411, 130 DLR (4th) 235, paras 113 and 118 wherein

pursuant to section 7 of the *Charter*'s protection of the right to life, liberty and security of the person.[484] In that judgement, the Court had to balance the competing values of dignity and the sanctity of life, showing it is possible to discuss and approach a *Charter* protection using the dignity standard. In *Reference re s. 94(2) of Motor Vehicle Act (British Columbia*), Justice Lamer explained that the principles of fundamental justice contained within section 7 of the *Charter* are derived from the "essential elements of a system for the administration of justice which is founded upon a belief in the dignity and worth of the human person".[485]

In addition to holding significance in our domestic laws, dignity is intimately linked to human rights in international law.[486] For example, the *United Nations Charter* sets out that each state must "reaffirm faith in fundamental human rights, in the dignity and worth of the human person".[487] In the *Universal Declaration of Human Rights*, the United Nations General Assembly pronounced that "[a]ll human beings are born free and equal in dignity and rights."[488] The preamble to the *International Covenant on Civil and Political Rights*, provides that the States which have ratified the Covenant shall recognize "the inherent dignity and … inalienable rights of all members of the human family" and that this recognition is "the foundation of freedom, justice and peace in the world".[489] It also states that human rights derive from "the inherent dignity of the human person".[490]

Justice L'Heureaux-Dube held that section 7 of the *Charter* protects a person's reasonable expectation of privacy in therapeutic records such that an infringement of that expectation would engage the liberty interest in section 7.
[484] 2015 SCC 5, [2015] 1 SCR 331 [*Carter*].
[485] [1985] 2 SCR 486, 24 DLR (4th) 536, para 71. See also *Carter*, para 81.
[486] Patrick Capps, *Human Dignity and the Foundations of International Law* (Oregon: Hart Publishing, 2010), page 107.
[487] [1945] CTS 7.
[488] [1948] GA Res 217, Article 1.
[489] [1976] CTS 47, 999 UNTS 171, preamble.
[490] *Ibid*, Article 10(1).

While dignity is a central tenant of our system of laws, it is a subjective idea. It fits well with the normative approach to section 8 in answering what protection we *should* expect from searches and seizures. Dignity is not measured positively through an assessment of the physical parameters of the search, i.e. if a search touches a person below their waistline or discloses medical information, it then infringes on their dignity. Dignity can instead be considered the permeating factor in deciding section 8 *Charter* claims and a central piece of the analysis, taking into account the specific context of technology in our society. Everyone has a right to dignity and it should not be infringed unreasonably. This clarity in purpose makes the analysis easier to implement; dignity would be given the utmost respect during police investigations, searches and seizures. The line between lawful and unlawful searches of technology would be when the search invades on the dignity of the person.

With the IoTs, we release information without retaining control over future dissemination of that information. We have little control over any information in our technology; it is both intentionally and unknowingly shared with corporations and the public. If the SCC recognizes section 8 protection beyond privacy, control can be eliminated as a consideration. Looking to the most recent authority from the SCC on section 8 in a technology case, *Marakah*, we see that the majority minimized the role of control in holding it was not dispositive and only one factor to be considered in the totality of the circumstances.[491] For this option of moving beyond privacy for section 8 protection, Chief Justice McLachlin's position for the majority in *Marakah* is a step in the right direction. The ideal analysis under this option would not place any weight on control as a factor or consideration because the reality is that we have very little control over our digital data. To maintain control as relevant, even as just one factor, does not appreciate the technological

[491] *Marakah*, para 44.

reality. Additionally, our future is likely to be a world where our actual control over our digital data will be even further diminished as corporations strive to gain more consumer data for direct marketing and customer acquisition.

With the current tools of analysis for determining a reasonable expectation of privacy removed from the equation (because privacy would not be the threshold consideration), many of the problems identified in chapter 4 would be eliminated. We would not have to resort to the biographical core to establish a sphere of information that deserves protection. The confusion surrounding the biographical core, what it entails and its usefulness in section 8 cases would no longer be relevant since the real issue would be a concern for the larger values protected by a revived section 8. The factors that make up the "totality of the circumstances" test would likely be relevant but not be as significant because the values at play, more than the search itself, would be central to the inquiry. While a new framework cannot stop the Court from leaving caveats and providing split decisions, it would remove the reasonable expectation of privacy analysis and the problems associated with it. When legislation is not adequately addressing a search or seizure issue, the expanded scope of section 8 to protect dignity could still provide protection of the interests at stake.

New problems may, and likely will develop but, at least, our *Charter* protections would not be restricted to constraints of privacy considerations. Until something is done to change our section 8 analysis, we will be left with unpredictability in how the SCC responds to search cases and how law enforcement should engage in investigations that intersect with technology. We should aim to go back to the basics of section 8 – prevent unreasonable searches and seizures.

5.6 CONCLUSION

This chapter outlined four options for the SCC to consider to better address searches of technology within section 8 of the *Charter*. Although there are likely a variety of potential other options for the Court moving forward, I believe that the four outlined above are the most realistic and achievable. The first option was to effectively do nothing and maintain the status quo. This option was quickly rejected because without any changes, the challenges identified in chapter 4 – incompetent analytical tools and uncertainty – will continue.

The section option was to embrace the risk analysis approach to privacy cases. This option will likely be considered the most controversial and undesirable, which is not surprising given the Court's constant rejection of the risk analysis and our society's general regard for privacy protection. This option was rejected because of the obvious contradiction with the high value placed on privacy by Canadians.

I suggested a spectrum of privacy protection as the third option for the Court to consider. The proposed three categories for technology were based upon intrusiveness, specificity, accuracy and the type of detail involved in the search. As the technology engaged becomes smarter and the detail more enlightening, the procedural requirements become more rigorous. A hypothetical scenario involving Mr. Criminal was used to illustrate the usefulness of the proposed categories. I believe that these categories would be advantageous for the Court when addressing emerging technologies, primarily because of the predictability it creates. I believe this is the most viable option of the Court moving forward within current section 8 jurisprudence. It requires some adaptation but no drastic changes to our understanding of the law of search and seizure.

The last option I outlined would see the most dramatic change made to section 8. Moving section 8 past the idea of individual privacy interests and toward a collective understanding of privacy based on dignity complements our ideals of privacy and our cultural respect for it. Section 8 is normatively orientated towards a fundamental respect for human dignity, making any transition to this option an easy one. The Court could draw upon its own references to dignity within past section 8 cases and its other *Charter* jurisprudence. This option is the best one for section 8 jurisprudence because it best fits our understanding of privacy and has the flexibility required to address the challenges the Court will inevitability face with emerging technologies involved in criminal investigations. However, more research would be required to adequately address the questions that naturally arise from the ideas expressed in this alternative proposal. Some of those questions include: How can an understanding of section 8 as a collective right help bring clarity and predictability to searches and seizures of technology? How would this understanding interact with the idea of dignity that underlies section 8 jurisprudence? How can the Court create normative yet concrete tools to judge when dignity is affected by a search and/or seizure? What would this look like in the reality of law enforcement efforts? Answering these questions is essential to developing this option for the Court and could certainly form the basis of another research project. The first step towards change is recognizing the possibility of viewing section 8 as a collective right and acknowledging the central place of dignity in any section 8 analysis.

CHAPTER 6: CONCLUSION

In early 2018, Chief Justice McLachlin responded to a question about privacy law at Dalhousie's Schulich School of Law by saying, "privacy, what privacy?"[492] She expressed her opinion that in our current age, there are huge threats to our privacy; people are less aware and have no control over where their information goes.

Technology has developed at a rapid pace within the last fifty years. It has become pervasive and almost inescapable. In 2014, Justice Karakatsanis in the dissenting judgement of *Fearon*, expressed that we "live in a time of profound technological change and innovation" and that technological developments "have revolutionized our daily lives".[493] We live in a society where mass data collection is a reality and its insecurity is alarming. Our culture has accepted surveillance, social media and the IoTs with open arms. When we embrace the IoTs, we invite technology to record our movements, daily activities, habits, and we ask it to predict when we need to change a light bulb or drink more water. We are handing over enormous amounts of information about ourselves to corporations and lose exclusive control over it. We realistically live in a world with very little privacy any longer; or at least significant practical challenges to privacy. The more technology becomes embedded in our lives, the smaller our sphere of real privacy becomes. Technology impacts criminal investigations; it has become a tool for committing crime and a tool for investigating crime. The aim of this thesis was to bring legal certainty to the use of technology in criminal investigations to answer the question: how can the line be drawn between lawful and unlawful searches?

[492] March 20, 2018.
[493] *Fearon*, para 100.

Section 8 of the *Canadian Charter of Rights and Freedoms* reads: "Everyone has the right to be secure against unreasonable search or seizure."[494] Privacy is the central idea for determining when a search or seizure is unreasonable. Searches or seizures will violate section 8 of the *Charter* when they invade a reasonable expectation of privacy. The Court has advocated for a normative and neutral approach that balances individual privacy with the interests of law enforcement. To do that they have created two primary tools of analysis – the biographical core and the totality of the circumstances. The SCC has held that section 8 should protect a biographical core of information that includes information that tends to reveal intimate details of the lifestyle and personal choices of an individual. However, this idea has seemingly lost prominence within the Court's jurisprudence and it is unclear what is included within the core. The totality of the circumstances test is meant to ensure that the context of a search is taken into consideration. Its current formulation includes four factors for consideration: the subject matter of the search, whether the claimant had a direct interest in the subject matter, whether the claimant had a subjective expectation of privacy in the subject matter and whether that expectation was objectively reasonable. The considerations under the totality of the circumstances test are heavily weighted toward the chosen definition of the subject matter which makes this test difficult to predict. The factors under the test are positive which creates a disconnect with the Court's stated intention of employing a normative analysis.

In addition to the challenges identified with the tools of analysis, chapter 4 highlights the problem with uncertainty prevalent in the current jurisprudence. The uncertainty is created by the Court's case-by-case approach to technology cases and compounded by their willingness to leave caveats and provide split decisions. Out of date legislation contributes to the problem even further

[494] *Charter*.

when it comes to technology that the law did not anticipate. As chapters 3 and 4 demonstrate, the current law on section 8 is problematic. The *Mills* case was used as an example to demonstrate how the challenges with section 8 jurisprudence are affecting real investigations and prosecutions.

As the SCC has stated, the rights enshrined in section 8 "must remain aligned with technological developments".[495] To remain aligned, the Court must appreciate our world of technology that has developed since the implementation of the *Charter* and since their decision in *Hunter v Southam*. Any new approach to section 8 must be sufficiently robust to protect a wide range of privacy interests yet provide law enforcement and the courts with sufficiently bright lines for determining what is and is not private. In chapter 5, I review four possible options for moving forward in an effort to bring legal certainty to section 8. The first two – maintain the status quo, adopt the risk analysis – were reviewed but quickly discarded as inappropriate for the development of the case law. The third option I considered was to employ a spectrum of privacy protection to address the data available through emerging technologies. This spectrum relies heavily on the SCC cases of the *M(A)* and *Kang-Brown* in the sniffer dog context but is modified and expanded for technological realities. I outlined three categories for technology based upon intrusiveness, specificity, accuracy and the type of detail involved in the search. Each category of technology would have specialized processes and requirements for searches requiring different levels of prior judicial authorization. The idea of using a spectrum of protection is nothing new, as is demonstrated by current legislative provisions. However, creating a spectrum specifically for technology is useful to provide clarity and predictability.

[495] *Telus*, para 33.

The last option proposed in chapter 5 is to move beyond the idea of individual privacy. I suggest adopting an understanding of privacy as a collective right and outlined how to reimagine the legal protection of privacy as a social value, primarily through expanded remedies for *Charter* breaches. In addition to this expanded view of privacy, I invite the Court to consider the genuine underlying concerns of section 8 – the freedom to live in dignity without fear of unreasonable search and seizure. Rather than rely on the current analytical tools with their limitations, the SCC can draw upon its own *Charter* jurisprudence and international legal principles to articulate dignity as the primary consideration in section 8 cases. There are remaining questions regarding this framework. For example, what normative analytical tools could be developed merits further elaboration. Whatever route is chosen for section 8 jurisprudence to move forward, the answer needs to promote predictability.

Searches and seizures of technology will inevitably continue. The borderless nature of electronic data, together with the fast-paced advancement of technology, means that Canada needs to find a sufficiently clear approach to section 8 of the *Charter* as soon as possible. Having an inadequate body of section 8 jurisprudence leaves Canadian law uncertain on where to draw the line between lawful and unlawful searches of technology. Perhaps comparative legal research could assist in defining clear parameters for searches of technology. Further research is necessary to find ways to achieve international harmonization.

Justice Rowe in *Marakah*, concurring with the majority, said: "principle and practically must not be strangers in the application of s. 8 or we might well thwart justice in the course of seeking to achieve it".[496] With the emerging IoTs and new technologies not yet known, the

[496] *Marakah*, para 89.

uncertainties prevalent within section 8 jurisprudence will become exacerbated. A section 8 approach based on dignity, prioritizing the prevention of *Charter* breaches, could provide certainty in criminal investigations and searches of technology.

BIBLIOGRAPHY

LEGISLATION

Canadian Charter of Rights and Freedoms, Part I of the *Constitution Act*, 1982, Schedule B to the *Canada Act 1982* (UK), 1982, c 11.

Controlled Drugs and Substances Act, SC 1996, c 19.

Corrections and Conditional Release Act, SC 1992, c 20.

Criminal Law Amendment Act, RSC 1985, c 27.

Criminal Code, RSC 1985, c C-46.

Customs Act, RSC 1985, c 1.

TREATIES

International Covenant on Civil and Political Rights, [1976] CTS 47, 999 UNTS 171.

United Nations Charter, [1945] CTS 7.

Universal Declaration of Human Rights, [1948] GA Res 217.

JURISPRUDENCE – CANADA

Canada (Director of Investigation & Research, Combines Investigation Branch) v Southam Inc., [1984] 2 SCR 145, 11 DLR (4th) 641.

Carter v Canada, 2015 SCC 5, [2015] 1 SCR 331.

Reference re s 94(2) of Motor Vehicle Act (British Columbia), [1985] 2 SCR 486, 24 DLR (4th) 536.

R v B (SA), 2003 SCC 60, [2003] 2 SCR 678.

R v Calderon [2004], 23 CR (6th) 1, 188 CCC (3d) 481.

R v Cole, 2012 SCC 53, 2012 SCC 53, [2012] 3 SCR 34.

R v Collins, [1987] 1 SCR 265, 33 CCC (3d) 1.

R v Dyment, [1988] 2 SCR 417, 66 CR (3d) 348.

R v Edwards, [1996] 1 SCR 128, 132 DLR (4th) 31.

R v Fearon, 2014 SCC 77, [2014] 3 SCR 621.

R v Gomboc, 2010 SCC 55, [2010] 3 SCR 211.

R v Jewitt, [1985] 2 SCR 128, 21 CCC (3d) 7.

R v Jones, 2017 SCC 60, [2017] 2 SCR 696.

R v Kang Brown, 2008 SCC 18, [2008] 1 SCR 456.

R v Law, 2002 SCC 10, [2002] 1 SCR 227.

R v M(A), 2008 SCC 19, [2008] 1 SCR 569.

R v Marakah, 2017 SCC 59, [2017] 2 SCR 608.

R v Mills, 2017 NLCA 12, [2017] 136 WCB (2d) 728.

R v Morelli, 2010 SCC 8, [2010] 1 SCR 253.

R v Morgentaler, [1988] 1 SCR 30, 37 CCC (3d) 449.

R v Oakes, [1986] 1 SCR 103, 24 CCC (3d) 321.

R v O'Connor, [1995] 4 SCR 411, 130 DLR (4th) 235.

R v Patrick, 2007 ABCA 308, [2007] 81 Alta LR (4th) 212.

R v Patrick, 2009 SCC 17, [2009] 1 SCR 579.

R v Plant, [1993] 3 SCR 281, 24 CR (4th) 47.

R v Sanelli, [1990] 1 SCR 30, 53 CCC (3d) 1.

R v Spencer, 2009 SKQB 341, [2009] 361 Sask R 1.

R v Spencer, 2011 SKCA 144, [2011] 377 Sask R 280.

R v Spencer, 2014 SCC 43, [2014] SCR 212.

R v Spencer, 2015 SKQB 62, [2015 469 Sask R 64.

R v Spencer, 2017 SKCA 54, [2017] SJ No 282.

R v Telus Communications Co., 2013 SCC 16, [2013] 2 SCR 3.

R v Tessling, 2004 SCC 67, [2004] 3 SCR 432.

R v Ward, 2012 ONCA 660, [2012] 112 OR (3d) 321.

R v Wise, [1992] 1 SCR 527, 11 CR (4th) 253.

R v Wong, [1990] 3 SCR 36, 1 CR (4th) 1.

R v Vu, 2013 SCC 60, [2013] 3 SCR 657.

JURISPRUDENCE – UNITED STATES

United States v Bynum, 604 F3d 161 (4th Cir 2010).

United States v Ferrell, 2016 WL 705197 (2016).

United States v Matish, 193 F Supp 3d 585, 2016 WL 3545776 (2017).

United States v Michaud, 2016 US Dist 11033, 2016 WL 337263.

United States v Perrine, 518 F3d 1196 (10th Cir 2008).

United States v Stults, 575 F3d 834 (8th Cir 2009).

United States v Werdene, 188 F Supp 3d 431, 2016 WL 3002376 (2016).

SECONDARY MATERIAL – ARTICLES

Addario, Frank and Andrew Burgess. "If You Don't Care about Privacy, Why Are You Wearing Pants?" (2015) 35:5 For the Defence – The Criminal Lawyers Association Newsletter.

Berghel, Hal. "Which is More Dangerous – the Dark Web or the Deep State?" Out of Band, Computer (July 2017).

Chan, Gerald. "Test Messaging: The Most Private (And Recorded) Form of Communication" (2018) 36 Adv J No 4.

Cockfield, Arthur. "Protecting the Social Value of Privacy in the Context of State Investigations using New Technologies" (2007) 40 UBC L Rev 41.

Cornell, Christopher. "*R. v. Spencer* and the Affirmation of Internet Privacy Rights in Canada" (2014) 20 L & Bus Rev Americas 649.

Coughlan, Stephen and Robert Currie. "Social Media: The Law Simply Stated" 11 Can J L & Tech 229.

Currie, Robert and Teresa Scassa. "New First Principles? Assessing the Internet's Challenges to Jurisdiction" (2011) 42 Geo J Intl L 1017.

DeFreitas, Hubbard and Magotiaux. "The Internet – Expectations of Privacy in a New Context" (2001-02) 45 Crim LQ 170.

Ducich, Stefan. "These Walls *Can* Talk! Security Digital Privacy in the Smart Home under the Fourth Amendment" (2017) 16 Duke Law & Tech Rev 278.

Gleicher, Nathaniel. "Neither a Customer Nor a Subscriber Be, Regulating the Release of User Information on the World Wide Web" (2008-09) 118 Yale LJ 1945.

Green, Tail and Grett Hughes. "Justice Abella on Privacy, Decision-Writing, and the Role of Law Schools" (2014) Ultra Vires October 29.

Hargreaves, Stuart. "*R v Gomboc*: Considering the Proper Role of the 'Biographical Core' in a Section 8 Informational Privacy Analysis" (2012) 59 CLQ 87.

Hunt, Angela. "Your TV May Be Spying on You" Law Technology News (November 25, 2013).

Hunt, Chris and Micah Rankin. "*R. v. Spencer*: Anonymity, The Rule of Law, and the Shriveling of the Biographical Core" (2015) 61 McGill L J 193.

Hutchinson, Terry and Nigel Duncan. "Defining and Describing What We Do: Doctrinal Legal Research" (2012) 17 Deakin LR 83.

Jochelson, Richard. "Trashcans and Constitutional Custodians: The Liminal Spaces of Privacy in the Wake of Patrick" (2009) 72 Sask L Rev 199.

Kirley, Elizabeth. "Can Twitter and BlackBerry Keep a Secret?" RegQuest (March 2011).

Nissani, Moti. "Ten Cheers for Interdisciplinarity: The Case for Interdisciplinary Knowledge and Research" (1997) 34 Soc Sci J 201.

Paton-Simpson, Elizbeth. "Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places" (2000) 50 Univ of Toronto LJ 305.

Phillips, Jim. "Why Legal History Matters" (2010) 41 VUWLR 293.

Pomerance, Renee. "Flirting with Frankenstein: The Battle between Privacy and Our Technological Monsters" (2016) 20 Can Crim LR 149.

Soper, Philip. "Legal Systems, Normative Systems, and the Paradoxes of Positivism" (1995) 8 Can J L & Juris 363.

Vogt, Sophia. "The Digital Underworld: Combating Crime on the Dark Web in the Modern Era" (2017) 15:1 Santa Clara JIL 104.

SECONDARY MATERIAL – BOOKS

Abelson, Hal, et al. *Blown to Bits: Your Life, Liberty, and Happiness After the Digital Explosion* (Toronto: Addison-Wesley, 2008).

Andrews, Lori. *I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy* (Toronto: Free Press, 2012).

Capps, Patrick. *Human Dignity and the Foundations of International Law* (Oregon: Hart Publishing, 2010).

Cryer, Robert, et al. *Research Methodologies in EU and International Law* (Oxford: Hart Publishing, 2011).

Fontana, James and David Keeshan, eds. *The Law of Search and Seizure in Canada*, 9th ed. (Toronto: LexisNexis Canada, 2015).

Hogg, Peter. *Constitutional Law of Canada* (Toronto: Carswell, 2015).

Kenyon, Andrew and Megan Richardson, eds. *New Dimensions in Privacy Law: International and Comparative Perspectives* (New York: Cambridge University Press, 2006).

Kirkpatrick, David. *The Facebook Effect: The Inside Story of the Company that is Connecting the World* (Toronto: Simon & Schuster, 2010).

Koch, Richard and Greg Lockwood. *Superconnect: The Power of Networks and the Strength of Weak Links* (London: Little Brown, 2010).

Krotoszynski, Ronald. *Privacy Revisited: A Global Perspective on the Right to be Left Alone* (Toronto: Oxford University Press, 2016).

Mayer-Schonberger, Viktor and Kenneth Cukier. *Big Data: A Revolution that will Transform how we Live, Work, and Think* (New York: Houghton Mifflin Harcourt Publishing Company, 2013).

McGrath, John. *Loving Big Brother: Performance, Privacy and Surveillance Space* (New York: Routledge, 2004).

McLean, Deckle. *Privacy and Its Invasion* (London: Praeger Publishers, 1995).

Mills, Jon. *Privacy the Lost Right* (New York: Oxford University Press, 2008).

O'Hara, Kieron and Nigel Shadbolt. *The Spy in the Coffee Machine: The End of Privacy as we Know It* (Oxford: One World Publications, 2008).

Ruff, Lori. *#Privacy Tweet: Addressing Privacy Concerns in the Day of Social Media* (California: THINKaha, 2010).

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

Stewart, Hamish. *Fundamental Justice: Section 7 of the Canadian Charter of Rights and Freedoms* (Toronto: Irwin Law Inc, 2012).

Stuart, Don. *Charter Justice in Canadian Criminal Law*, 6th ed. (Toronto: Carswell, 2014).

Vaidhyanathan, Siva. *The Googlization of Everything (And Why We Should Worry)* (Los Angeles: University of California Press, 2011).

Vamosi, Robert. *When Gadgets Betray Us: The Dark Side of our Infatuation with New Technologies* (New York: Basic Books, 2011).

Van Dijck, Jose. *The Culture of Connectivity: A Critical History of Social Media* (New York: Oxford University Press, 2013).

Waldo, James, et al. *Engaging Privacy and Information Technology in a Digital Age* (Washington: The National Academies Press, 2007).

Whitaker, Reg. *The End of Privacy: How Total Surveillance is Becoming a Reality* (New York: The New Press, 1999).

Zittrain, Jonathan. *The Future of the Internet - and How to Stop It* (London: Yale University Press, 2008).

SECONDARY MATERIAL – MULTIMEDIA

Banking on Bitcoin, (Netflix, documentary: August 14, 2017).

Cybercrime with Ben Hammersky, (Netflix, television series: September 1, 2015).

Inside the Dark Web, (BBC Worldwide Ltd., documentary film: 2014).

Supreme Court of Canada Webcast, *Spencer*, online: http://www.scc-csc.ca/case-dossier/ info/webcastview-webdiffusionvue-eng.aspx?cas=34644&id=2013/2013-12-09--34644&date=2013-12-09&fp=n&audio=n.

Supreme Court of Canada Webcast, *Mills*, online: https://www.scc-csc.ca/case-dossier/info/webcastview-webdiffusionvue-eng.aspx?cas=37518&id=2018/2018-05-25--37518&date=2018-05-25&audio=n.

Wisdom of the Crowd (Global TV, television series: October 1, 2017).

SECONDARY MATERIAL – ONLINE SOURCES

ABC. "Extreme Weight Loss", "Grey's Anatomy", "Scandal", "The Bachelor", "The Bachelorette", "Bachelor in Paradise" online: http://abc.go.com/shows/.

Amazon. "Alexa and Alexa Device FAQs" online: https://www.amazon.com/gp/help/customer/display.html?nodeId= 201602230.

Amazon. "Alexa Terms of Use" online: https://www.amazon.com/gp/help/customer/display.html?nodeId= 201809740.

Amazon. "Echo" online: https://www.amazon.ca/echo.

Amazon. "Echo & Alexa Devices" online: https://www.amazon.com/Amazon-Echo-And-Alexa-Devices/b?ie=UT F8&node=9818047011.

Barlow, John Perry. "A Declaration of the Independence of Cyberspace" (February 8, 1996) online: https:// www.eff.org/cyberspace-indepen dence.

BBC. "Facebook Scandal 'hit 87 million users'" (April 4, 2018) online: www.bbc.com/news/technology-43649018.

BBC. "NHS cyber-attack: GPs and Hospitals hit by Ransomware" (May 13, 2017) online: www.bbc.com/news/health-39899646.

BBC. "Uber Concealed Huge Data Breach" (November 22, 2017) online: www.bbc.com/news/technology-42075306.

Bloomberg. "2016 was a Record Year for Data Breaches" (January 19, 2017) online: https://www.bloomberg.com/news/articles/2017-01-19/data-breaches-hit-record-in-2016-as-dnc-wendy-s-co-hacked.

Bravo. "Million Dollar Listing", "Real Housewives of Atlanta", "Real Housewives of Beverly Hills", "Real Housewives of New York", "Real Housewives of Orange County", "Real Housewives of Potomac", "Real Housewives of Vancouver", "Real Housewives of Toronto", "Vanderpump Rules", online: http://www.bravotv.com/.

Business Insider. "Amazon's Alexa won Christmas this Year" (December 26, 2017) online: http://www.businessinsider.com/amazon-alexa-top-ios-android-app-christmas-day-echo-sales-2017-12.

Canadian Association of Chiefs of Police. "Resolutions adopted at the 111th Annual Conference" (Ottawa, Ontario: August 2016) online: https://www.cacp.ca/resolution.html?asst _id=1197.

Canadian Tire. "Nest" Products online: http://www.canadiantire.ca/en/nest.html.

CBC. "Canadians Among Top Participants on Illegal Drug Website" (August 16, 2012) online: http://www.cbc.ca/news/canada/canadians-among-top-participants-on-illegal-drug-website-1.1158116.

CBC. "Couple finds out Wife is Pregnant, Thanks to Fitbit (and Reddit)" (February 12, 2016) online: http://www.cbc.ca/radio/asithappens/as-it-happens-friday-edition-1.3445891/couple-finds-out-wife-is-pregnant-thanks-to-fitbit-and-reddit-1.3445900.

CBC. "CRTC Declares Broadband Internet Access a Basic Service" (December 21, 2016) online: http://www.cbc.ca/news/politics/ crtc-internet-essential-service-1.3906664.

CBC. "Equifax Data Breach a 'Digital Disaster' for Canadians" (September 17, 2017) online: http://www.cbc.ca/news/canada/new-brunswick/nb-opinion-equifax-data-breach-1.4293609.

CBC. "Google Sister Company makes 'Bold Bet' with new Tech-focused Neighbourhood 'Sidewalk Toronto'" (October 17, 2017) online: http://www.cbc.ca/news/ canada/toronto/waterfront-toronto-announcement-1.4358683.

CBC. "Hackers Threaten to Reveal Personal Data of 90,000 Canadians caught in Bank Hack" (May 29, 2018) online: www.cbc.ca/news/business/bank-hack-tuesday-1.4682018.

CBC. "Internet Users' Privacy Upheld by Canada's Top Court" (June 13, 2014) online: http://www.cbc.ca/news/technology/internet-users-privacy-upheld-by-canada-s-top-court-1.2673823.

CBC. "Khalid Masood reportedly used WhatsApp minutes before London Attack" (March 26, 2017) online: http://www.cbc.ca/news/world/social-media-terrorism-whatsapp-encryption-1.4041574.

CBC. "Murdered Woman's Fitbit Logged Steps after Husband said she Died" (April 25, 2017) online: http://www.cbc.ca/news/technology/fitbit-murder-1.4084506.

CBC. "Ransomware Attack Reveals Bitcoin as an Accessory to Cybercrime: Don Pittis" (May 16, 2017) online: http://www.cbc.ca/news/business/ransomware-bitcoin-threat-cyberattack-1.4115344.

CBC. "RCMP need Warrantless Access to online Subscriber Info: Paulson" (November 25, 2015) online: http://www.cbc.ca/news/politics/paulson-rcmp-subscriber-info-warrantless-access-1.3337028.

CBC. "State-sponsored Cyberattacks on Canada successful about Once a Week" (October 30, 2017) online: www.cbc.ca/news/politics/cyber-attacks-canada-cse-1.4378711.

CBC. "The Villain, the Faithful Romantic: Big Brother casting call Draws all Types" (September 23, 2017) online: http://www.cbc.ca/news/canada/ saskatoon/villain-moral-centre-big-brother-6-saskatoon-1.4304427.

CBC. "What You Need to Know about Canada Revenue Agency's 'Internet Vulnerability'" (March 14, 2017) online: www.cbc.ca/news/technology/canada-revenue-agency-cra-internet-vulnerability-bug-apache-struts-2-1.4023838.

CBC. "Welcome to the Neighbourhood. Have You Read the Terms of Service?" (January 16, 2018) online: http://www.cbc.ca/news/technology/smart-cities-privacy-data-personal-information-sidewalk-1.4488145.

CBC. "Your Smart Fridge could be Mining Bitcoins for Criminals" (June 29, 2018) online: https://www.cbc.ca/news/technology/bitcoin-hacking-smart-devices-1.4728222.

CBS. "CSI Cyber", "Madam Secretary", "Survivor", "Wisdom of the Crowd" online: https://www.cbs.com/shows/.

CNBC. "Amazon's Alexa had a Breakout Holiday – People even used Echoes to buy more Echoes" (December 26, 2017) online: https://www.cnbc.com/2017/12/26/how-many-amazon-alexa-echoes-were-sold-over-the-2017-holidays.html.

CNBC. "Amazon Echo Secretly Recorded a Family's Conversation and Sent it to a Random Person on their Contact List" (May 24, 2018) online: https://www.cnbc.com/2018/05/24/ amazon-echo-recorded-conversation-sent-to-random-person-report.html.

CNBC. "In the Wake of the Equifax Data Breach, Consumers More at Risk" (March 11, 2018) online: https://www.cnbc.com/2018/03/10/in-the-wake-of-the-equifax-data-breach-consumers-more-at-risk.html.

CNN. "Cops Use Murdered Woman's Fitbit to Charge her Husband" (April 26, 2017) online: https://www.cnn.com/2017/04/25/us/fitbit-womans-death-investigation-trnd/index.html.

CNN. "Every single Yahoo account was hacked – 3 billion in all" (October 4, 2017) online: http://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html.

CNN. "Half of American Adults Hacked this Year" (May 28, 2014) online: http://money.cnn.com /2014/05/28/ technology/security/hack-data-breach/index.html.

CNN. "Target Hack is a Wake-Up Call on Privacy" (January 11, 2014) online: http://money.cnn.com/2014/01/11/technology/security/target-hack-privacy/index.html?iid=EL.

CTV. "Designated Survivor" online: https://www.ctv.ca/designated-survivor.

CTV. "'Erie' Music, Man's Voice Creeps into Nursery after Baby Monitor Hacked" (July 23, 2015) online: https://www.ctvnews.ca/canada/eerie-music-man-s-voice-creeps-into-nursery-after-baby-monitor-hacked-1.2483170.

Dratel, Joshua. Letter (November 19, 2013) online: http://www.libertyunderattack.com/wp-content/uploads/2015/ 06/131119-Letter-Submitted-in-Support-of-Application-for-Ross-Bail.pdf.

Dr. Phil. "Dr. Phil" online: https://www.drphil.com/.

Evans, Dave. "The Internet of Things: How the Next Evolution of the Internet is Changing Everything" (CISCO Internet Business Solutions Group, 2011), online: www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411 FINAL.pdf.

Facebook. "Newsroom" online: https://newsroom.fb.com/company-info/.

Federal Trade Commission. FTC Staff Report "Internet of Things: Privacy & Security in a Connected World" (January, 2015) online: www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-novem ber-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

Fitbit. "Shop Versa" online: https://www.fitbit.com/en-ca/shop/versa.

Food Network, "Top Chef", "Iron Chef", "Chef School" and "Chopped" online: www.foodnetwork.ca/shows/.

Forbes. "An Interview with a Digital Drug Lord: The Silk Road's Dread Pirate Roberts (Q&A)" (August 14, 2013) online: https://www.forbes.com/sites/andygreenberg/2013/08/14/an-interview-with-a-digital-drug-lord-the-silk-roads-dread-pirate-roberts-qa/#32088c3a5732.

Forbes. "An NSA Cyber Weapon might be Behind a Massive Global Ransomware Outbreak" (May 12, 2017) online: https://www.forbes.com/sites/thomasbrewster/2017/05/12/nsa-exploit-used-by-wannacry-ransomware-in-global-explosion/#735792bde599.

Forbes. "Meet the Dread Pirate Roberts, the Man Behind Booming Black Market Drug Website Silk Road" (August 14, 2013) online: https://www.forbes.com/sites/andygreenberg/2013/08/14/meet-the-dread-pirate-roberts-the-man-behind-booming-black-market-drug-website-silk-road/.

Forbes. "What are the Biggest Challenges facing the Cybersecurity Industry?" (September 15, 2017) online: https://www.forbes.com/sites/quora/2017/09/15/what-are-the-biggest-challenges-facing-the-cybersecurity-industry/#4b41cbc72d62.

Gawker. "The Underground Website where you can Buy Any Drug Imaginable" (June 1, 2011) online: http://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160.

Geist, Michael. "Supreme Court Delivers Huge Victory for Internet Privacy & Blows Away Government Plans for Reform" (June 13, 2014) online: http://www.michaelgeist.ca/2014/06/scc-spencer-decision/.

Global. "Big Brother", Bull" online: https://www.globaltv.com/.

Google. "Data Security & Privacy on Google Home" online: https://support.google.com/googlehome/answer/707 2285?hl=en.

Google. "Google Home" online: https://store.google.com/ca/product/google_home.

Harvard University. "Cybersecurity: Managing Risk in the Information Age", online: https://gs.harvardx.harvard.edu/harvard-cybersecurity-online-short-course-hm/?&ef_id=c:263435404471_d:c_n:g_ti:kwd-358401477327_p:_k:%2Bcyber%20%2Bsecurity_m:b_a:56898363791&gclid=EAIaIQobChMIq8Lb88jR2gIVBEsNCh0cuwyKEAMYASAAEgK8CvD_BwE.

HGTV. "Love it Or List It Vancouver", "Property Brothers", "Property Virgins" online: www.hgtv.ca/shows/.

Historica Canada. "Heritage Minutes – Marshall McLuhan" online: https://www.historicacanada.ca/content/heritage-minutes/marshall-mcluhan.

Huffington Post. "Parental Warning: Your Baby Monitor can be Hacked" (August 24, 2017) online: https://www.huffingtonpost.com/healthline-/parental-warning-your-bab__b_11668882.html.

LG. "LG OLED TV AI ThinQ" online: https://www.lg.com/ca_en/oled-tv/AI.jsp?cmpid=2018HQSEM_TV_CI-EN_Smart-AI-Generic_Exact-0628_Smart-TV_k3598&gclid=CjwKCAjw7IbaBRBqEiwA6AyZguPZAtfmG1Wq-DK2T8Z67onav3kxYa511LfRWGY4mlKBhdtwBXVTxoC2mAQAvD_BwE#intro.

LG. "Refrigerators" online: https://www.lg.com/ca_en/refrigerators?cmpid=2018HA-SEM_CI_Google_Refrigerator-1806-EN_Smart_k0149pc&gclid=CjwKCAjw7IbaBRBqEiwA6AyZgpG57m1N18 -6WJeNbf-whsyBtwl_EQas5_xh23HDzxUjlxE2_ywt2xoC8T8QAvD_BwE.

Los Angeles Times. "Facebook: Reaction in the Twittersphere" (May 18, 2012) online: http://articles.latimes.com/2012/may/18/business/la-fi-tn-facebook-reaction-twitter-20120518.

Merriam-Webster. "Normative" online: https://www.merriam-webster.com/dictionary/normative.

Motherboard. "The Canadian Supreme Court Just Stood up for Online Privacy Rights" (June 13, 2014) online: https://motherboard.vice.com/en_us/article/4x3n3j/the-canadian-supreme-court-just-stood-up-for-privacy-rights.

NBC News. "More than 4 Billion Data Records were Stolen Globally in 2016" (January 30, 2017) online: https://www.nbcnews.com/storyline/hacking-in-america/more-4-billion-data-records-were-stolen-globally-2016-n714066.

Oxford Dictionaries. "Word of the Year 2009" online: https://en.oxforddictionaries.com/word-of-the-year/word-of-the-year-2009.

Oxford English Dictionary. "A Heads Up for the June 2013 OED Release" online: https://public.oed.com/the-oed-today/recent-updates-to-the-oed/previous-updates/june-2013-update/a-heads-up-for-the-june-2013-oed-release/.

Quartz. "An Oregon Family's Encounter with Amazon Alexa Exposes the Privacy Problem of Smart Home Devices" (May 25, 2018) online: https://qz.com/1288743/amazon-alexa-echo-spying-on-users-raises-a-data-privacy-problem/.

RCMP. "About the RCMP" (May 7, 2018) online: http://www.rcmp-grc.gc.ca/aboutausujet/ index-eng.htm.

RCMP. "National Child Exploitation Coordination Centre" online: http://www.rcmp-grc.gc.ca/ncecc-cncee/about-ausujet-eng.htm.

Sidewalk Labs. "Submission" (October 17, 2017) online: https://sidewalktoronto.ca/wp-content/uploads/2017/10/ Sidewalk-Labs-Vision-Sections-of-RFP-Submission.pdf.

Sleep Number. "Explore the Sleep Number 360 Smart Bed" online: https://www.sleepnumber.com/360.

The Economist. "Plant of the Phones" (February 26, 2015) online: https://www. economist.com/news/leaders/21645180-smartphone-ubiquitous-addictive-and-transformative-planet-phones.

The Globe and Mail. "Equifax Data Breach could become the Most Costly in Corporate History" (March 2, 2018) online: https://www.theglobeandmail.com/report-on-business/international-business/us-business/equifax-data-breach-could-become-the-most-costly-in-corporate-history/article38180834/.

The Globe and Mail. "Hackers target Canadian Government's Energy and Resource Departments" (November 17, 2016) online: https://www.theglobe andmail.com/news/politics/ hackers-target-governments-energy-and-resource-departments/article32890960/.

The Guardian. "John Perry Barlow Obituary" (February 11, 2018) online: https://www.theguardian.com/technology/2018/feb/11/john-perry-barlow-obituary.

The Guardian. "Man Suspected in Wife's Murder after her Fitbit data Doesn't Match his Alibi" (April 25, 2017) online: https://www.theguardian.com/technology/2017/apr/25/fitbit-data-murder-suspect-richard-dabate.

The New York Times. "Facebook Privacy: A Bewildering Tangle of Options" (May 12, 2010) online: https://archive.nytimes.com/www.nytimes.com/interactive/2010/05/12/business/facebook-privacy.html.

The Star. "Equifax finds additional 2.4 Million in US impacted by 2017 Data Breach" (March 1, 2018) online: https://www.thestar.com/business/economy/2018/03/01/equifax-finds-additional-24-million-in-us-impacted-by-2017-data-breach.html.

The Star. "More than 600,000 Canadians caught in Facebook Data Scandal" (April 4, 2018) online: https://www.thestar.com/news/canada/2018/04/04/more-than-600000-canadians-caught-in-facebook-data-scandal.html.

The Star. "StatsCan Hacked after Government Sites made Vulnerable: Officials" (March 13, 2017) online: https://www.thestar.com/news/canada/2017/03/13/statscan-hacked-after-government-sites-made-vulnerable-officials.html.

The Star. "Uber says 815,000 Canadians affected by Data Breach as Formal Investigation Opened" (December 11, 2017) online: https://www.thestar.com/business/2017/12/11/privacy-commissioner-to-investigate-uber-data-breach .html.

The United States Attorney's Office, Southern District of New York, "Manhattan U.S. Attorney Announces The Indictment of Ross Ulbricht, the Creator and Owner of the "Silk Road" Website"

(February 4, 2014) online: https://www.justice.gov/ usao-sdny/pr/manhattan-us-attorney-announces-indictment-ross-ulbricht-creator-and-owner-silk-road.

The Wall Street Journal. "More Cyberattack Victims Emerge as Agencies Search for Clues" (May 13, 2017) online: https://www.wsj.com/articles/more-cyberattack-victims-emerge-as-agencies-search-for-clues-1494671938.

The World Bank. "World Bank Group and GSMA Announce Partnership to Leverage IoT Big Data for Development" (February 26, 2018) online: http://www.worldbank.org/en/news/press-release/2018/02/26/world-bank-group-and-gsma-announce-partnership-to-leverage-iot-big-data-for-development.

Time Magazine. "Death of Privacy" (August 25, 1997) online: http://content.time.com/time/covers/0,16641,19970825,00.html.

Time Magazine. "Person of the Year" (December 25, 2006) online: http://content.time.com/time/covers/0,16641, 20061225,00.html.

TLC. "90-day fiancé", "Fat Chance", "Kate plus Eight", "My 600 lb Life", "My Big Fat Fabulous Life", "Say Yes to the Dress", "Sister Wives", "Skin Tight", "The Spouse House", "Trading Spaces", online: https://www.tlc.com/tv-shows/.

TOR. "TOR: Onion Service Protocol" online: www.torproject.org/docs/hidden-services.html.en.

TOR. "TOR: Overview" online: https://www.torproject.org/about/overview.html.en.

Twitter. "home page" online: https://twitter.com/?lang=en.

Twitter. "How to Use Media Studio" online: https://help.twitter.com/en/using-twitter/media-studio.

United Nations Office on Drugs and Crime. "Comprehensive Study on Cyber Crime: Chapter 2 The Global Picture" (February 2013) online: https://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/ CYBER CRIME_STUDY_210213.pdf.

Vumetric. "Cyber Security for Industry 4.0" https://www.vumetric.com/en/industries/manufacturing/.

Wareable. "Best Heart Rate Monitors: Top Watches, Chest Straps and Fitness Trackers" online: https://www.wareable.com/fitness-trackers/best-heart-rate-monitor-and-watches.

WhatsApp, "WhatsApp" online: https://www.whatsapp.com/.

Wired. "Hackers are Exploiting Baby Monitors, But We Know How to Stop Them" (October 15, 2013) online: http://www.wired.com/gadgetlab/2013/10/baby-monitor-hacking/.

Wired. "The Biggest Cybersecurity Disasters of 2017 So Far" (July 1, 2017) online: https://www.wired.com/story/2017-biggest-hacks-so-far/.

Wired. "Internet of Things: Where does the Data Go?" online: https://www.wired.com/insights/2015/03/internet-things-data-go/.

Wired. "The Ransomware Meltdown Experts Warned about is Here" (May 12, 2017) online: https:// www.wired.com/2017/05/ransomware-meltdown-experts-warned/.

Wired. "UN Report Declares Internet Access a Human Right" (June 3, 2011) online: https://www.wired.com/2011/06/internet-a-human-right/.

Wired. "Yahoo's 2013 email Hack actually Compromised Three Billion Accounts" (October 3, 2017) online: https://www.wired.com/ story/yahoo-breach-three-billion-accounts/.

YouTube. "About" online: https://www.youtube.com/yt/about/.

YouTube. "For Press" online: https://www.youtube.com/intl/en/yt/about/press/.

YouTube. "Twitter Explained" online: https://www.youtube.com/watch?v=RoHhNisGMk8.

YouTube. "YouTubers React to Top 10 Most Viewed YouTube Videos of All Time" online: https://www.youtube.com/watch?v=gcOQumLbvXI.

SECONDARY MATERIAL – OTHER

House of Commons, Report of the Standing Committee on Access to Information, Privacy and Ethics, *Privacy and Social Media in the Age of Big Data* (April 2013) from *Minutes of Proceedings: Evidence*, 1st Session, 41st Parliament (June 12, 2012) 1230.

Public Safety Canada. *Horizontal Evaluation of Canada's Cyber Security Strategy – Final Report* (September 29, 2017).