ARTICLE

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

Lee-Ann Conrod *

CITED: (2019) 24 *Appeal* 115

ABSTRACT

Technology has changed our world, including how crimes are committed and how law enforcement investigate them. Many of our daily activities, criminal or otherwise, leave behind digital data. Vast amounts of specific and accurate information is collected through our intentional uses of technology and our inadvertent interactions with it. This paper examines how section 8 of the *Charter* is adapting to new technologies through the SCC's jurisprudence. The current body of section 8 jurisprudence from the SCC has provided neither the desired certainty nor predictability. I point out some specific challenges with section 8 law and propose a new way forward: a spectrum of protection.

INTRODUCTION

Criminals and law enforcement alike rely on ever more sophisticated technologies in their respective pursuits. Some criminals employ new technologies to avoid police detection in novel ways, for instance, by using cryptocurrencies to hide the proceeds of crime. Other criminals employ technology in the commission of their offences, for instance, by accessing child pornography on the internet or making drug and weapons trafficking arrangements via text messages on smartphones. In the same way technology provides criminals with means and methods to commit crimes, it can provide specific and accurate information about activities that would assist law enforcement in their investigations. Today, more crimes than ever are inadvertently leaving behind digital data in the form of IP addresses, search history or electronic records of the criminal activities.

This paper examines how technology has become a valuable and desirable component of many criminal investigations and makes proposals for appropriately regulating search and seizure powers. To investigate and prosecute an accused person with the aim of achieving a conviction, the police must have gathered the evidence lawfully so that it is

* Lee-Ann received her JD in 2010 and her LLM in 2018. She is currently a Crown Prosecutor with the Public Prosecution Service of Canada in the Atlantic Regional Office. The views expressed in this article are those of the author alone.

admissible at trial. The *Charter*[1] limits law enforcement's ability to search technology and seize information. Section 8 provides that "[e]veryone has the right to be secure against unreasonable search or seizure."[2]

While the text 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 message conversations.[8] The SCC 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 that the purpose of section 8 is 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 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.[11] Protecting an individual's technological privacy from the State in the context of a criminal investigation is complex. The central focus of this paper 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*? Throughout this paper, I will show that given the challenges with the current jurisprudence, the law should be modified to establish greater legal certainty.

First, I discuss the current technological context and explore how new technological tools are used to commit crimes. Second, I outline the development and current state of the law on section 8 of the *Charter* and elucidate the serious deficiencies in the law dealing with search and seizure issues in the context of technology. Third, I assess the effectiveness of the framework currently in place for section 8 of the *Charter*. This section also explores contextual factors surrounding the interpretation of section 8 with a view to examining the major challenges to achieving certainty within this area of the law. I outline a variety of ways in which the SCC has added to the uncertainty. Fourth, and lastly, I recommend 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: a spectrum of protection. That spectrum would be assessed using four criteria: intrusiveness, specificity and accuracy of

---

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

2 *Charter*, *supra* note 1, s 8.

3 *R v Wise*, [1992] 1 SCR 527 [*Wise*].

4 *R v Plant*, [1993] 3 SCR 281 [*Plant*]; *R v Gomboc*, 2010 SCC 55 [*Gomboc*].

5 *R v Tessling*, 2004 SCC 67 [*Tessling*].

6 *R v Morelli*, 2010 SCC 8 [*Morelli*].

7 *R v Cole*, 2012 SCC 53 [*Cole*].

8 *R v Fearon*, 2014 SCC 77 [*Fearon*]; *R v Marakah*, 2017 SCC 59 [*Marakah*]; *R v Jones*, 2017 SCC 60 [*Jones*].

9 *Canada (Director of Investigation & Research, Combines Investigation Branch) v Southam Inc.*, [1984] 2 SCR 145 [*Hunter v Southam*] at paras 16, 18-19, and 26. See also Don Stuart, *Charter Justice in Canadian Criminal Law*, 6th ed. (Toronto: Carswell, 2014) [Stuart] at 290.

10 *Ibid* at paras 25 and 27.

11 See for example *Gomboc*, *supra* note 4; *R v M(A)*, 2008 SCC 19 [*M(A)*]; *R v Kang-Brown*, 2008 SCC 18 [*Kang-Brown*].

the search, and the type of detail revealed. In this paper, I describe three categories along the spectrum which demonstrate the usefulness of this approach.

I. THE USE OF TECHNOLOGIES IN CRIMINAL INVESTIGATIONS

A. A Brief History of Technology

Technology is ever evolving, and its use 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 less than 50 years old. The personal computer was developed in the 1970s[12] and in 1979 a protocol was created that allowed computers to link together over the telephone which "grew together into a network of all networks, the internet."[13] At that time, no one imagined today's network connecting hundreds of millions of computers around the globe. In 1978, the first satellites were launched for the Global Positioning System (GPS).[14] In the 1990s, email began to be used by the general public.[15]

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.[16] The internet has had a considerable impact 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.[17] Therefore, it is no surprise that technology is having an impact on crime—both its conduct and detection.

B. The Position of Social Media

One cannot fully and accurately review the influence of technology in today's culture without mentioning social media.[18] The norms for sociality have drastically changed for an entire generation who understand social media as a regular part of our existence. The

---

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

13 *Ibid* at 54. See also Jonathan Zittrain, *The Future of the Internet - and How to Stop It* (London: Yale University Press, 2008) at 36 for a description of the growth of the internet.

14 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) at 88.

15 David Kirkpatrick, *The Facebook Effect: The Inside Story of the Company that is Connecting the World* (Toronto: Simon & Schuster, 2010) [Kirkpatrick] at 67.

16 Whitaker, *supra* note 12 at 47. See also *Morelli*, 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," at para 114. See also Hal Abelson, et al, *Blown to Bits: Your Life, Liberty, and Happiness After the Digital Explosion* (Toronto: Addison-Wesley, 2008) at 4 for discussion of digital explosion.

17 See Robert Currie and Teresa Scassa, "New First Principles? Assessing the Internet's Challenges to Jurisdiction" (2011) 42 Geo J Intl L 1017 at 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> archived at <https://perma.cc/9K7L-LJ9W> where Jean-Pierre Blais, CRTC's Chair stated that the internet is a vital service, essential to life and success. See also Wired, "UN Report Declares Internet Access a Human Right" (June 3, 2011) online: <https://www.wired.com/2011/06/internet-a-human-right/> archived at <https://perma.cc/6QGJ-PVPE>.

18 Social media is internet based, interactive platforms that allow for multi-party live communication. See Stephen Coughlan and Robert Currie, "Social Media: The Law Simply Stated" 11 Can J L & Tech 229 at 230.

social impact of this form of media is immeasurable. Facebook, Twitter, YouTube, and many other social media platforms have created a new reality wherein people are connected on a global and instantaneous basis. 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."[19] Facebook caused a shift in the boundaries of personal privacy with many users willingly displaying intimate details of their lives.[20]

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. For instance, sexual predators use social media platforms to find and communicate with vulnerable children. Increased frequency of online child exploitation has led to the development of a specialized unit of the RCMP.[21] Likewise, police are now using social media to investigate and capture internet predators.

C. The Internet of Things

The so-called "Internet of Things" ("IoTs") will likely form the next frontier for criminals and law enforcement disputes for the SCC to consider with respect to section 8 analysis.[22] The IoTs generally refers to devices other than computers, smartphones or tablets that transmit data through the internet. The IoTs is creating and collecting data within our homes, traditionally considered one of the most private spaces. There are now a tremendous number of "things" connected to the internet. The IoTs has become common to many Canadian households in the form of wearable technology,[23] connected automation systems,[24] and many other common household devices.[25] The World Bank is even hoping to use big data from the IoTs to help end extreme poverty and fuel economic growth.[26]

The IoTs gathers large quantities of information about our private activites, preferences, and habits to optimize the function of a device.[27] We regularly face encroachments on our privacy in exchange for perceived positive benefits we get from handing over our personal

19 Kirkpatrick, *supra* note 15 at 15.

20 *Ibid* at 200-201 and see 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.

21 The National Child Exploitation Coordination Centre deals exclusively with "investigations related to the sexual exploitation of children on the internet in Canada", see RCMP, "National Child Exploitation Coordination Centre" online: <http://www.rcmp-grc.gc.ca/ncecc-cncee/about-ausujet-eng.htm> archived at <https://perma.cc/484K-YHWL>.

22 See The Economist, "Planet of the phones" (February 26, 2015) online: <https://www.economist.com/news/leaders/21645180-smartphone-ubiquitous-addictive-and-transformative-planet-phones> archived at <https://perma.cc/RS7D-TWEV> for how the smart phone has changed society.

23 Such as smart watches, fitness trackers and medical devices.

24 Such as adjusting light bulbs, coffee machines, music players and temperature controls. 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) [O'Hara] at 8-9.

25 For examples see: regarding smart TVs: Angela Hunt, "Your TV May Be Spying on You," Law Technology News (November 25, 2013); Canadian Tire, "Nest" Products online: <http://www.canadiantire.ca/en/nest.html> archived at <https://perma.cc/99TP-HUMN> that describes Nest products as "more than smart—they're thoughtful." See also, Fitbit, "Shop Versa" online: <https://www.fitbit.com/en-ca/shop/versa> archived at <https://perma.cc/69YN-R85V> for details on "a health & fitness smartwatch that lasts 4+ days and features 24/7 heart rate, phone-free music, apps, coaching & more." See generally, O'Hara, *supra* note 24.

26 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> archived at <https://perma.cc/Q86B-GXTJ>.

27 Wired, "Internet of Things: Where does the Data Go?" online: <https://www.wired.com/insights/2015/03/internet-things-data-go/> archived at <https://perma.cc/QLG5-88JU>.

information.[28] 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. 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.[29] That activity can be monitored to establish the resident's patterns. While a fridge's data cannot precisely determine a person's routine, it can be used to gather a composition of information. Law enforcement could use the data to verify surveillance observations or to help determine the best time to conduct a covert entry into the home to gather the physical evidence needed to further an investigation.[30]

Smart devices can easily be used as tools of invasive surveillance. These different devices have varying levels of data intrusion, from the mundane to the extremely personal.[31] 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. Yet, the lawfulness of police seizures of data from IoTs remains uncertain and has the potential to be contested.

D. Technological Tools for Crime

Technology facilitates new crimes and changes how traditional crimes are committed. 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.

These crimes may be perpetrated on the "surface web," that is, websites indexed by search engines.[32] In addition to the surface web, there is a layer of the internet called the "deep web" and beyond there is 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.[33] The "dark web," like the "deep web", is not indexed and is designed to operate and be accessed anonymously.[34] 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.[35] This "rising popularity of encryption" makes law enforcement efforts in

28 Whitaker, *supra* note 12 at 135.

29 O'Hara, *supra* note 24 at 14-15.

30 Fitbit has even been partially credited with solving a murder investigation, see 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> archived at <https://perma.cc/TT97-PHXB>.

31 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> archived at <https://perma.cc/KL7L-LRSC>.

32 Hal Berghel, "Which is More Dangerous—the Dark Web or the Deep State?" Out of Band, Computer (July 2017) [Berghel] at 86.

33 *Ibid* at 86.

34 See TOR, "TOR: Onion Service Protocol" online: <www.torproject.org/docs/hidden-services.html.en> archived at <https://perma.cc/RF83-6CLW>. Other examples include: I2P, Freenet, Riffle, Hidemyass.com. See also *Cybercrime with Ben Hammersky*: Season 1, Episode 1 (Netflix, television series: September 1, 2015).

35 Berghel, *supra* note 32 at 87.

searches of technology increasingly difficult.[36] Criminals often use cryptocurrency online to further ensure their anonymity. Cryptocurrency is virtual money that is untraceable. While it has legal uses, cryptocurrency has essentially become "the new hidden suitcase full of unmarked bills."[37] The dark web, together with cryptocurrencies, has made digital black markets on the dark web possible.[38] In addition to the internet, communication technology assists criminals in evading law enforcement. Encryption services or those where messages auto-delete and video conversations that cannot be captured are becoming more commonplace.[39] Remote Administration Tools (RATs) are designed to allow a user to control their devices remotely. A criminal could easily benefit from such technology, for instance, by remotely erasing incriminating evidence on a seized device. There is seemingly an entire market available for online criminal activity.

Technology allows tech savvy criminals to conduct their activities differently. Police must 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. 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 these technologies.[40] Searches of these new technologies and seizures of information will continue to increase. How can law enforcement ensure those searches and seizures are lawful? Jurisprudence from section 8 of the *Charter* should provide guidance.

II. UNREASONABLE SEARCH AND SEIZURE UNDER SECTION 8 OF THE *CHARTER*

The *Canadian Charter of Rights and Freedoms* forms part of the *Constitution of Canada, 1982*, which constitutes "the supreme law of Canada."[41] The *Charter* requires a flexible interpretation that can adapt to changes over time, including changing societal values.[42] The SCC in *Hunter v Southam* specifically adopted this flexible interpretation for section 8 of the *Charter*.[43] In the unanimous judgment, Justice Dickson (as he then was) in explained that section 8 "must be capable of growth and development over time to meet

---

36 Sophia Vogt, "The Digital Underworld: Combating Crime on the Dark Web in the Modern Era" (2017) 15:1 Santa Clara JIL 104 at 114.

37 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> archived at <https://perma.cc/QH9J-8LAQ>. Some well-known cryptocurrencies are: Bitcoin, Litecoin, Peercoin, Ripple, Zcash, Feathercoin, etc.; see *Banking on Bitcoin* (Netflix, documentary: August 14, 2017).

38 *Ibid*.

39 Examples include: PGP, Skype, Telegram, WhatsApp, Hushmail, Cryptocat. See for example <https://telegram.org/> archived at <https://perma.cc/AYU3-VTE6> which promotes itself as a messaging application where "messages are heavily encrypted and can self-destruct."

40 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> archived at <https://perma.cc/Z6Y5-2WT7>. See also, WhatsApp website which brags about their services encryption capabilities: WhatsApp, "WhatsApp" online: <https://www.whatsapp.com/> archived at <https://perma.cc/475X-GFFW>.

41 *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.

42 See *Hunter v. Southam*, *supra* note 9 at para 16. See also Peter Hogg, *Constitutional Law of Canada*, Student Edition (Toronto: Carswell, 2015), at 36-25 to 36-26 [Hogg].

43 *Hunter v Southam, supra* note 9.

new social, political, and historical realities often unimagined by its framers."[44] The SCC identified the purpose of section 8 as to *prevent* unjustified state intrusion on individual privacy.[45] 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.[46] In *R v Cole*, Justice Fish plainly stated that "[p]rivacy is a matter of reasonable expectations."[47] A diminished expectation of privacy is still reasonable and attracts section 8 *Charter* protection, subject to intrusion only with lawful authority.[48] Where there is an intrusion on any reasonable expectation of privacy, the state action will be considered a "search" for section 8 purposes.[49] 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?[50] 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?[51] *Hunter v Southam* established prior authorization as a "precondition for a valid search and seizure."[52] While there are some situations which allow for warrantless searches, such as searches incident to lawful arrest, the SCC established a minimum standard for lawful searches. 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.[53] 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.[54] Alternatively, a warrantless search attracts a presumption of unreasonableness.[55] This system of prior authorization, instead of after-the-fact validation, avoids promoting a justification mentality for law enforcement. 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.

---

44 *Ibid* at para 16. To achieve this flexibility, section 8 of the *Charter* should be given a "broad, purposive analysis," see *Hunter v Southam*, *supra* note 9 at paras 18-19 and 26; see also Stuart, *supra* note 9 at 290. *Hunter v Southam* continues to be a seminal judgement for section 8 cases as it recognized an "individual's right to privacy," see *Hunter v Southam*, *supra* note 9 at para 32. James Fontana and David Keeshan, eds. *The Law of Search and Seizure in Canada*, 9th ed (Toronto: LexisNexis Canada Inc., 2015) [Fontana] at 4.

45 *Hunter v Southam*, *supra* note 9 at paras 25 and 27.

46 *Ibid* at para 25; *Gomboc*, *supra* note 4 at para 20.

47 *Cole*, *supra* note 7 at para 35.

48 *Tessling*, *supra* note 5 at para 42; *Cole*, *supra* note 7 at 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, *supra* note 44 at 21-24.

49 *Hunter v Southam*, *supra* note 9 at para 25. See also Stuart, *supra* note 9 at 295.

50 Fontana, *supra* note 44 at 4.

51 *R v Edwards*, [1996] 1 SCR 128 at para 33; *Jones*, *supra* note 8 at para 11.

52 *Hunter v Southam*, *supra* note 9 at para 29; see also paras 27 and 28.

53 *R v Collins*, [1987] 1 SCR 265 at para 34.

54 *Criminal Code*, RSC 1985, c C-46 [*Criminal Code*], s 487; *Gomboc, supra* note 4 at para 20.

55 *Hunter v Southam*, *supra* note 9 at para 30. See also Fontana, *supra* note 44 at 5.

Once it has been established that there is a reasonable expectation of privacy, the task of any section 8 analysis is to balance competing values: individual interests and rights against collective preferences and desire for security. Section 8 of the *Charter* "is concerned with the degree of privacy needed to maintain a free and open society."[56] 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.[57]

The SCC has explained that the balance is a "delicate"[58] one between privacy and law enforcement interests that must be "calibrated according to the circumstances."[59] The competing values involved are interrelated[60] and the weight placed on these values changes over time.[61] 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.

III. CHALLENGES WITH THE CURRENT INTERPRETATION OF SECTION 8 OF THE *CHARTER*

A. Uncertainty Inherent within Section 8

The SCC has repeatedly acknowledged that while the language of section 8 may be simple, it is inherently imprecise.[62] 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."[63] *Hunter v Southam* recognized that the guarantee provided by section 8 is "vague and open."[64] This permits flexibility but at the cost of certainty.[65] 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.[66] These are extremely difficult terms to define with precision.[67]

The concept of privacy is constantly evolving and has blurred "reasonableness" boundaries.[68] 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.

---

56 *R v Ward*, 2012 ONCA 660 at para 86.

57 *Hunter v Southam*, *supra* note 9 at para 25.

58 *Marakah*, *supra* note 8 at paras 100 and 114.

59 *Kang-Brown*, *supra* note 11 at para 24.

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

61 See *R v Spencer*, 2014 SCC 43 [*Spencer*] at para 15; *Fearon*, *supra* note 8 at paras 112-125.

62 See for example, *Hunter v Southam*, *supra* note 9 at paras 15-16; *Tessling*, *supra* note 5 at para 25; *M(A)*, *supra* note 11 at para 39; *R v Patrick*, 2009 SCC 17 [*Patrick*] at paras 14 and 29.

63 *M(A), supra* note 11 at para 5.

64 *Hunter v Southam*, *supra* note 9 at para 15.

65 Hogg, *supra* note 42 at 36-39.

66 *Tessling*, *supra* note 5 at para 25. See also Fontana, *supra* note 44 at 18.

67 Ronald Krotoszynski, *Privacy Revisited: A Global Perspective on the Right to be Left Alone* (Toronto: Oxford University Press, 2016), at xi. See also Jon Mills, *Privacy the Lost Right* (New York: Oxford University Press, 2008) at 4. See also *Tessling*, *supra* note 5 at para 25, Fontana, *supra* note 44 at 18.

68 *Hunter v Southam*, *supra* note 9 at para 25.

Philosophical approaches to the study of privacy have focused on normative questions around whether privacy is a right, a good in itself, or an instrumental good.[69] Economic approaches to privacy have centered around the economic value of privacy.[70] Sociological approaches have emphasized the ways in which the collection and use of personal information reflect and reinforce relationships of power.[71] 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 transferable to another fact scenario. And what is "private" in one context will not necessarily be considered private in another.[72] In assigning meaning to these terms, judges "will inevitably be influenced by their own social, economic and political values."[73] 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 that greatly impact the protection afforded by section 8 to all Canadians.[74]

B. Case-by-Case Approach and Caveats

The purpose of section 8 is to prevent unjustified state intrusions before they happen.[75] This preventative purpose is effectively disregarded by the SCC when they allow for caveats and adopt a case-by-case approach. For 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.[76]

The evidence in each case may determine the lawfulness of the search, but without more direction, it leaves the legal parameters of the search inexact. Similarly, in 2013, 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.[77]

He did not go on to clarify in what scenario this may be possible, and it is unclear why he would prescribe such a caveat in that case. This statement creates uncertainty about whether a general warrant can authorize prospective production of future text messages. As a result, law enforcement may erroneously apply a prospective general warrant. Again, in *Vu*, Justice Cromwell declined 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

69 James Waldo, et al. *Engaging Privacy and Information Technology in a Digital Age* (Washington: The National Academies Press, 2007) at 1.

70 *Ibid* at 55. Economics and privacy also consider: consumer valuation of privacy, markets for privacy, the impact of state privacy and data security regulation on companies.

71 *Ibid* at 79.

72 For example, a file on a personal computer within one's home would attract a reasonable expectation of privacy (see *R v Vu*, 2013 SCC 60 [*Vu*]), but a similar file on a work computer in a public space attracts a diminished expectation of privacy (see also *Cole, supra* note 7).

73 Hogg, *supra* note 42 at 36-9.

74 *Patrick*, *supra* note 62 at paras 14 and 29.

75 *Hunter v Southam*, *supra* note 9 at para 27.

76 *M(A)*, *supra* note 11 at para 88 [emphasis added].

77 *R v Telus Communications Co*, 2013 SCC 16 [*Telus*] at para 107 [emphasis added].

> a range of situations and *it will not always be appropriate to require specific, prior judicial authorization* before they can search those devices.[78]

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. In *Fearon*, Justice Cromwell for the majority again missed the opportunity to establish a clear legal rule for cell phone searches incident to arrest.[79] More recently in 2017, in *Marakah*, former Chief 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.[80]

Further in her reasons, she provided that not every electronic communication will attract a reasonable expectation of privacy. Especially problematic is the statement that "different facts may well lead to a different result." [81] This is the opposite of a clear, preventative approach to section 8. The continual allowance for caveats leaves an absence of bright lines for police to respect. The Court cannot practically expect law enforcement to consistently prevent unjustified searches before they happen without clarity in the law. Lower courts are left with no clear guidance to decipher section 8 search issues on a case-by-case basis. Litigants will continue to argue opposing yet equally rational 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.[82]

C. Split Decisions Leave Confusion

The seemingly straightforward text of section 8 of the *Charter* has proven to be highly contentious. Justices at the SCC are often divided in their reasons[83] and litigants are regularly joined by interveners[84] expressing disagreement on the issues. It seems as though developing technology has added to the confusion.[85]

---

78 *Vu*, *supra* note 72 at para 63 [emphasis added].

79 *Fearon*, *supra* note 8 at para 84.

80 *Marakah*, *supra* note 8 at para 5 [emphasis in original].

81 *Ibid* at para 55.

82 See *Cole supra* note 7, *Vu supra* note 72, and *Fearon supra* note 8.

83 SCC has released split judgments throughout its history on section 8 cases. See for example *R v Dyment*, [1988] 2 SCR 417, split 3:2:1; *R v Wong*, [1990] 3 SCR 36, split 4:2:1; *Kang-Brown*, *supra* note 11; *M(A)*, *supra* note 11, both split 4:2:2:1; *Gomboc*, *supra* note 4, split 4:3:2; *Telus*, *supra* note 77, split 3:2:2; *Fearon*, *supra* note 8, split 4:3; *Markaha*, *supra* note 8, split 4:2:1; and *Jones*, *supra* note 8, split 5:1:1.

84 See for example *Spencer*, *supra* note 61, with 6 interveners; *Fearon*, *supra* note 8, with 9 interveners; *Marakah*, *supra* note 8, with 7 interveners; *Jones*, *supra* note 8, with 6 interveners; and *R v Mills*, 2017 NLCA 12, leave to appeal to SCC granted February 10, 2017, with 9 interveners.

85 See for example *Telus*, *supra* note 77, dealing with text messages, split 3:2:2; *Fearon*, *supra* note 8, dealing with search of a cell phone incident to arrest, split 4:3; *Marakah*, *supra* note 8, dealing with sent text messages, split 4:2:1; and *Jones*, *supra* note 8, dealing with a production order for past text messages, split 5:1:1.

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.[86] 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. Former 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 electricity consumption records without a warrant—but by different routes. However, a different split is found when considering the use of the "biographical core."[87] Justice Deschamps used the biographical core as a yardstick for determining whether there was a reasonable expectation of privacy, 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 former 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.[88] Split judgements reflect indecisiveness from the SCC. The lack of clarity from Canada's top court denies law enforcement clear direction. To achieve the goal of *preventing* unjustified searches, we require clarity in the law. Continued strong divisions from the SCC about how to approach section 8 claims make it difficult for Crown and defense to advise their clients and for Canadians to know the limits of law enforcement. If defense and Crown counsel lack clear direction, more litigation and less case resolution results, further crowding already overburdened courts.

It is difficult to follow section 8 case law development and predict the outcome of an issue with such a lack of certainty. Therefore, it is a challenge to prevent a breach 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 the law. How is the Court going to handle new technology coming when they cannot even agree how to treat utility

86 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.

87 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. A biographical core of information was first discussed by the SCC in 1993 in the *Plant* case, *supra* note 4. 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. In *Tessling*, *supra* note 5, the biographical core of information was central in the SCC's assessment. *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 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. 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 at 210, where the authors describe the concept of the biographical core as an "unwieldy concept."

88 *Kang-Brown*, *supra* note 11 at para 19.

records?[89] With emerging IoTs and new technologies, these problems will only become exacerbated. They may even get worse before they get better if the SCC does not recognize their own inconsistency in approaches to technological section 8 cases.

IV. MAKING SENSE OF SECTION 8 FOR SEARCHES OF NEW TECHNOLOGIES: A SPECTRUM OF PRIVACY PROTECTION

In this section, I outline an option for the SCC to consider—a spectrum of privacy protection for section 8 cases dealing specifically with technology. This proposal is closely aligned with and builds upon current jurisprudence. 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"[90] may issue a search warrant but an interception for private communications requires a judge[91] of the superior court, unless there is a consent to the interception.[92] Certain warrants require that the authorization be applied for by the Attorney General instead of simply a peace officer.[93] 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"[94] to "reasonable grounds to suspect."[95] After certain warrant-specific preconditions have been met, 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.[96] There are recognized exceptions to the requirements of prior judicial authorization such as customs border searches, search incident to arrest, circumstances of urgency, and dog sniffer searches.[97] In this way, the law already recognizes

89 See *Gomboc*, *supra* note 4 (split 4:3:2).

90 In section 2 of the *Criminal Code*, *supra* note 54 "justice" is defined as "a justice of the peace or a provincial court judge."

91 In section 552 of the *Criminal Code*, "judge" is defined as "a judge of the superior court of criminal jurisdiction in the Province." See section 185 of the *Criminal Code, supra* note 54 for details of the Application for a Part VI Authorization.

92 See section 184.2 of the *Criminal Code, supra* note 54.

93 See for example section 185 of the *Criminal Code*, *supra* note 54 setting out requirements for an application for authorization to intercept private communications, which requires the application made and signed by the Attorney General, the Minister of Public Safety and Emergency Preparedness, or an agent specially designated.

94 See section 184 for authorization to intercept private communications; section 487 for search warrant; section 487.01 for general warrant; and section 487.014 for production order.

95 See section 487.015 for production order to trace specified communication; section 487.016 for production order—transmission data; section 487.017 for production order—tracking data; and section 487.018 for production order—financial data. Part VI of the *Criminal Code, supra* note 54 sets out a comprehensive scheme for the interception of private communications, which requires more than "reasonable grounds to believe". See section 185(1)(h) for investigative necessity requirement and see (1.1) for exception for criminal organizations and terrorist groups.

96 Note in section 185 of the *Criminal Code*, *supra* note 54 there is an exception to this requirement for offences related to criminal organizations and terrorist groups.

97 Fontana, *supra* note 44 at 6. See also *Kang-Brown*, *supra* note 11, and *M(A)*, *supra* note 11, for the standard of reasonable suspicion for sniffer dogs, border crossings (*Customs Act, supra* note 48, s 98), and 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*, *supra* note 54 which allows the warrantless interception of private communications in exigent circumstances to prevent serious harm.

a continuum of constitutionally valid standards for privacy protection.[98] 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 different degrees of privacy online.[99] A spectrum of privacy protection with different levels of justification and procedural requirements based on the level of privacy implicated would match this reality. As Justice Binnie noted in *M(A)*, all searches "do not have the same invasive and disruptive quality."[100] 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 standard was "pragmatic and balanced"[101] 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 the search did not interfere with bodily integrity.[102] 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.[103]

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 technological devices. 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.[104] 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 not likely that this particular technology 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.[105] A continuum of protection recognizes that our interactions with different technological devices is not uniform and that our privacy may in fact fall at different places on that spectrum. Applying this idea to the IoTs requires us to answer questions such as: when an authorization is required, who can apply for it and grant it, and what, if any, conditions

98 See *Kang-Brown*, *supra* note 11 at para 169.

99 Lori Ruff, *#Privacy Tweet: Addressing Privacy Concerns in the Day of Social Media* (California: THINKaha, 2010) at 22.

100 *M(A)*, *supra* note 11 at para 13.

101 *Kang-Brown*, *supra* note 11 at para 166.

102 *Ibid* at para 242.

103 *Ibid* at paras 234-238.

104 See *Fearon*, *supra* note 8 at paras 54 and 63.

105 *Kang-Brown*, *supra* note 11 at para 220.

attach 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.

I propose a spectrum of privacy protection for the Court to consider employing in section 8 cases dealing with technology. I suggest 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 criterium 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.

A. 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.[106] 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 determine whether someone who lives in a rural area is home at a particular time, the information from their fridge and light bulbs could help. In many cases, it is not feasible to drive right up to the house to look for themselves without the risk of being detected, so if the data tells them that the fridge door was opened 5 minutes ago, and the lights are on, they can make an informed assumption that someone is home.

Any search to obtain data from a dumb device would be minimally intrusive, specific, and have pinpoint accuracy.[107] 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, and causes no inconvenience nor interference 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 restricted because no other information would be obtained. For instance, 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 much like they did the forward looking infrared ("FLIR") or digital recording ammeter ("DRA"). Like FLIR, the information "may or may not be capable of giving rise to an inference about what was actually going on inside."[108] And similar to DRA, the information disclosed is

106 O'Hara, *supra* note 24 at 14-16.

107 Note that I have adapted these three considerations from the sniffer dog cases of *M(A)*, *supra* note 11 and *Kang-Brown*, *supra* note 11.

108 *Tessling*, *supra* note 5 at para 27.

not of an intimate or private nature, is not confidential like a doctor-patient relationship, and nor does it disclose political affiliation, sexual orientation, etc. of the user.[109] These devices in Category 1 provide a pattern of use of a device.

A discussion of this category would not be complete without addressing former 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.[110]

The difference with smart devices is that they are entirely optional, unlike electricity use in the case of DRA data. They are nice to have as a luxury but smart devices are not "essential" to our lives. Having the newest technology embedded in our homes is a newer trend. That may change in the next decade but for now former 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 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.[111]

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*,[112] 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,[113] 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 and include investigative delays and more paperwork for judges. Realistically, if police are contemplating

---

109 See *Gomboc*, *supra* note 4 at para 7.

110 *Ibid* at para 100.

111 *Kang-Brown*, *supra* note 11 at para 75.

112 See *Kang-Brown*, *supra* note 11 at para 60.

113 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; and section 487.018, Production Order for financial data.

searching a Category 1 device, they will also likely be seeking to search devices under Category 2 and/or Category 3, which I propose would require judicial authorization. To require prior authorization for Category 1 searches that engage relatively minor privacy interest would unduly contribute to our already overburdened courts.

B. Category 2—Technology that Potentially Reveals Sensitive Information

I propose that the devices in this category are those that disclose 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. In addition to the tracking function,[114] these devices capture details about a user's life. For example, smart watch devices and smart beds record and store information about the user's heart rate and sleep patterns.[115] 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. The technology in 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 matches that for devices that track an individual's movements within the *Criminal Code*[116] and its use makes sense as we move towards 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.[117]

C. 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 that can listen and respond to us. Smart televisions with cameras, microphones, speakers, and digital assistants such as Amazon's Alexa would be included in this category. These devices have the ability to surreptitiously listen to our daily ramblings and record massive amounts of information about us that

---

114 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.

115 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> archived at <https://perma.cc/X3W6-FJM7>. For beds, see Sleep Number, "Explore the Sleep Number 360 Smart Bed" online: <https://www.sleepnumber.com/360> archived at <https://perma.cc/PJX9-UYSG> advertising that the bed "knows how you're sleeping" with SleepIQ technology inside the bed to track how well you sleep each night.

116 *Criminal Code*, *supra* note 54, s 492.1(2).

117 The reason I propose emulating the tracking provision found in section 492.1(2) of the *Criminal Code*, *supra* note 54 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.).

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.[118] 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 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 what was said during an intercepted conversation: it includes data such as an individual's location when they were talking, the duration for which they spoke, to whom they were talking, and more. 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 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 an expansion of the definition of private communications within the *Criminal Code* 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.[119]

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*.[120]

---

118 Part VI of the *Criminal Code*, *supra* note 54 specifically deals with invasions of privacy. It defines what is an invasion of privacy, how to legally obtain an authorization to legally intercept a private communication and creates a complete process and procedure for doing so.

119 *Criminal Code*, *supra* note 54, s 183.

120 *Telus*, *supra* note 77 at paras 49 and 67.

As Justice Binnie noted in *Tessling*, the reasonableness of the search has to be determined by looking at current, not potential, technology capabilities.[121] A device may transition from Category 1 to Category 2 or even 3. It is not hard to imagine 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. Such an approach would create more predictability than simply saying any evolution in the future will be dealt with by the courts on a case by case basis, as was done in *Tessling*.[122]

This spectrum approach acknowledges that not all technology is the same and does not provide the same information. Nor should it attract the same privacy protection: one cannot use the 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.

CONCLUSION

In early 2018, former Chief Justice McLachlin responded to a question about privacy at Dalhousie's Schulich School of Law by asking "privacy, what privacy?"[123] She expressed her opinion that in our current age, there are huge threats to our privacy; she explained that 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."[124] We live in a society where mass data collection is a reality and its insecurity is alarming to many. Our culture has accepted surveillance, social media and the Internet of Things with open arms. When we embrace the IoTs, we invite technology to record our movements, daily activities, and 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 in the process. We realistically live in a world with very little privacy, or at least significant practical challenges to privacy. The more technology becomes embedded in our lives, the smaller our sphere of real privacy becomes. In particular, technology impacts criminal investigations: it has become a tool for committing crime and a tool for investigating crime.

As the SCC has stated, the rights enshrined in section 8 "must remain aligned with technological developments."[125] To remain aligned, the Court must appreciate our world of technology that has developed since the implementation of the *Charter* and since the Supreme Court 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 clear lines for determining what is and is not private.

In this paper, I have suggested a spectrum of privacy protection for the Court to consider. The three proposed categories for technology are 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 should become

121 *Tessling*, *supra* note 5 at paras 29 and 55.

122 *Ibid*.

123 Former Chief Justice McLachlin, (Address delivered at Dalhousie Schulich School of Law, 20 March 2018) [unpublished].

124 *Fearon*, *supra* note 8 at para 100.

125 *Telus*, *supra* note 77 at para 33.

more rigorous. I believe that these categories would aid the Court in addressing emerging technologies, primarily due to the predictability it creates. It requires some adaptation but no drastic changes to our understanding of the law of search and seizure.

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. As Justice Rowe in *Marakah* said, concurring with the majority: "principle and practicality must not be strangers in the application of s. 8 or we might well thwart justice in the course of seeking to achieve it."[126] As this paper identifies, there is a lack of practical direction from the Court—principled or otherwise. With the emerging IoTs and new technologies not yet known, the uncertainties prevalent within section 8 jurisprudence will become exacerbated unless clear guidelines are adopted by the SCC.

126 *Marakah*, *supra* note 8 at para 89.