McGill Law Journal
Revue de droit de McGill

Criminal Law and Digital Technologies: An Institutional Approach to Rule Creation in a Rapidly Advancing and Complex Setting

Colton Fehr

Volume 65, Number 1, September 2019

URI: https://id.erudit.org/iderudit/1074418ar
DOI: https://doi.org/10.7202/1074418ar

See table of contents

Publisher(s)

McGill Law Journal / Revue de droit de McGill

ISSN

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

Explore this journal

Cite this article

Fehr, C. (2019). Criminal Law and Digital Technologies: An Institutional Approach to Rule Creation in a Rapidly Advancing and Complex Setting. *McGill Law Journal / Revue de droit de McGill*, *65*(1), 67–113. https://doi.org/10.7202/1074418ar

Article abstract

Courts and legislatures in Canada and around the world have struggled to respond effectively and efficiently to the challenges posed by the use of rapidly advancing and complex technologies. As a result, scholars have debated the appropriate role of each institution with respect to governing privacy in the digital age. This debate has provided foundational evidence upon which to develop a normative framework for governing digital privacy. Yet, the Canadian literature has only sparsely addressed the ability of Canadian legislatures to respond to the challenges presented by the use of digital technologies. This article begins to fill the gap in the literature by asking whether Parliament has been able to reply to the use of complex and rapidly advancing technologies in an efficient, coherent, and fair manner. I conclude that Parliament's legislative framework for governing state intrusions into digital privacy has been patchwork and inconsistent. After comparing these findings to the literature on the relative institutional capacity of courts, I outline a general strategy for ensuring each institution tasked with governing digital privacy is working to its strengths, not its weaknesses.

McGill Law Journal — Revue de droit de McGill

Criminal Law and Digital Technologies: An Institutional Approach to Rule Creation in a Rapidly Advancing and Complex Setting

*Colton Fehr**

Courts and legislatures in Canada and around the world have struggled to respond effectively and efficiently to the challenges posed by the use of rapidly advancing and complex technologies. As a result, scholars have debated the appropriate role of each institution with respect to governing privacy in the digital age. This debate has provided foundational evidence upon which to develop a normative framework for governing digital privacy. Yet, the Canadian literature has only sparsely addressed the ability of Canadian legislatures to respond to the challenges presented by the use of digital technologies. This article begins to fill the gap in the literature by asking whether Parliament has been able to reply to the use of complex and rapidly advancing technologies in an efficient, coherent, and fair manner. I conclude that Parliament's legislative framework for governing state intrusions into digital privacy has been patchwork and inconsistent. After comparing these findings to the literature on the relative institutional capacity of courts, I outline a general strategy for ensuring each institution tasked with governing digital privacy is working to its strengths, not its weaknesses.

Les tribunaux et législatures au Canada et à travers le monde ont eu de la difficulté à répondre de manière efficace et efficiente aux défis posés par l'utilisation de technologies qui sont complexes et se développent rapidement. Par conséquent, les chercheurs ont débattu du rôle approprié de chaque institution dans l'encadrement de la protection de la vie privée à l'ère numérique. Ce débat a fourni des preuves fondamentales pour construire un cadre normatif pour la gouvernance du respect de la vie privée numérique. Néanmoins, la littérature canadienne n'a traité la capacité des législatures canadiennes à répondre aux défis présentés par l'utilisation des technologies numériques que de manière éparse. Cet article est un premier pas pour combler ces lacunes dans la littérature en analysant la capacité du Parlement à répondre à l'utilisation de technologies qui sont complexes et se développent rapidement de façon efficace, cohérente et équitable. Nous concluons que le cadre législatif du Parlement pour régir les intrusions de l'État dans la vie privé numérique des citoyens a été un assemblage décousu d'initiative législative. Après avoir comparé ces constats avec la littérature sur la capacité institutionnelle relative des tribunaux, nous présentons une stratégie générale visant à assurer que chaque institution chargée de réglementer la vie privé numérique s'appuie sur ses forces et non ses faiblesses.

* Assistant Professor, Simon Fraser University, School of Criminology. I wish to thank Steven Penney, James Stribopoulos, Eric Adams, and the external reviewers for their comments on earlier drafts of this article.

Citation: (2019) 65:1 McGill LJ 67 — Référence : (2019) 65:1 RD McGill 67

Introduction

In *United States v. Jones*,[1] Justice Alito observed that "[i]n the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical."[2] Given the limited resources of government, storing mass amounts of data or conducting regular surveillance of everyday activities was not economically feasible. With the onset of the digital age, this reality was thoroughly undermined.[3] Both government and corporate entities now frequently employ rapidly advancing and complex technologies, which permit the gathering and storing of incredible amounts of information about individuals.[4]

This novel legal terrain has given rise to a general debate in the American literature about whether courts or legislatures are institutionally better equipped to meet the challenges presented by technological advancement.[5] Courts have been shown to have two main weaknesses. First, the rapid evolution of digital technologies often results in judges rendering outdated decisions.[6] Second, because of the "unusually complex" nature of digital technologies, judges operating within the adversarial system often receive inadequate evidence upon which to develop principled rules.[7] This is unsurprising since there is no guarantee that the parties to a proceeding have sufficient technological knowledge or resources to explain the intricacies of a complex technology.[8] Legislatures are arguably better equipped to

---

1 565 US 400 (2012), Alito J concurring [*US v Jones*].

2 *Ibid* at 12. In the Canadian context, see *R v Tessling*, 2004 SCC 67 at para 16 [*Tessling*].

3 See *US v Jones*, *supra* note 1 at 12–13.

4 See *R v Spencer*, 2014 SCC 43 at para 46 [*Spencer*].

5 The key works include Orin S Kerr, "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution" (2004) 102:5 Mich L Rev 801 [Kerr, "Fourth Amendment"]; Daniel J Solove, "Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference" (2005) 74:2 Fordham L Rev 747 [Solove, "Fourth Amendment"]; Erin Murphy, "The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions" (2013) 111:4 Mich L Rev 485; David Alan Sklansky, "Two More Ways Not to Think About Privacy and the Fourth Amendment" (2015) 82:1 U Chicago L Rev 223.

6 See Kerr, "Fourth Amendment", *supra* note 5 at 868–69; Daniel M Scanlan, "Issues in Digital Evidence and Privacy: Enhanced Expectations of Privacy and Appellate Lag Times" (2012) 16:3 Can Crim L Rev 301 at 312 [Scanlan, "Issues"].

7 See Stephen Breyer, "Our Democratic Constitution" (2002) 77:2 NYUL Rev 245 at 261. See also Kerr, "Fourth Amendment", *supra* note 5 at 875–77; Scanlan, "Issues", *supra* note 6 at 302.

8 See generally Kerr, "Fourth Amendment", *supra* note 5 at 875.

respond given their greater informational capacity and ability to pass laws expediently.[9]

Others counter, however, that in practice legislatures are often unable or unwilling to update "obviously flawed and outdated provisions."[10] These difficulties are explained by identifying structural impediments to passing legislation, as well as special interest influence on legislatures, including majoritarian influence stemming from a dislike of criminal suspects.[11] Even though judges tend to craft broad rules to give future courts flexibility in assessing novel circumstances, judicial rule-making at least allows for the incremental, evolutionary development of policy in response to changing technological and social circumstances.[12] As a result, these scholars argue that courts are better suited to govern privacy interests in complex search technologies.[13]

The Canadian literature has identified similar problems with respect to judicial governance of digital technologies.[14] Unfortunately, however,

---

9 See generally *ibid* at 870–75; Breyer, *supra* note 7 at 261–64; *Riley v California*, 573 US 373 (2014) at 6, Alito J; Marc Jonathan Blitz, "Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity" (2004) 82:6 Tex L Rev 1349 at 1421.

10 Murphy, *supra* note 5 at 533. See also Sklansky, *supra* note 5 at 227–28; Solove, "Fourth Amendment", *supra* note 5 at 763–67; Donald A Dripps, "Constitutional Theory for Criminal Procedure: *Dickerson*, *Miranda*, and the Continuing Quest for Broad-but-Shallow" (2001) 43:1 Wm & Mary L Rev 1 at 4, 46.

11 See Sklansky, *supra* note 5 at 227; Murphy, *supra* note 5 at 535–36. As discussed below, others deny that lobbying has a significant impact in the criminal and digital contexts. See e.g. Kerr, "Fourth Amendment", *supra* note 5 at 885.

12 See Murphy, *supra* note 5 at 535–36.

13 See e.g. Sklansky, *supra* note 5 at 223–24; Solove, "Fourth Amendment", *supra* note 5 at 761. See also Daniel J Solove, *Nothing to Hide: The False Tradeoff Between Privacy and Security* (New Haven: Yale University Press, 2011) ch 17; Christopher Slobogin, *Privacy at Risk: The New Government Surveillance and the Fourth Amendment* (Chicago: University of Chicago Press, 2007) at 201–03; William J Fenrich, "Common Law Protection of Individuals' Rights in Personal Information" (1996) 65:3 Fordham L Rev 951 at 958.

14 See e.g. Scanlan, "Issues", *supra* note 6; Steven Penney, "Reasonable Expectations of Privacy and Novel Search Technologies: An Economic Approach" (2007) 97:2 J Crim L & Criminology 477 [Penney, "Reasonable Expectations"]; Susan Magotiaux, "Out of Sync: Section 8 and Technological Advancement in Supreme Court Jurisprudence" (2015) 71 SCLR (2d) 501; Jordan Fine, "Leaving Dumb Phones Behind: A Commentary on the Warrantless Searches of Smart Phone Data Granted in *R v Fearon*" (2015) 13:2 CJLT 171; Colton Fehr & Jared Biden, "Divorced from (Technological) Reality: A Response to the Supreme Court of Canada's Reasons in *R v Fearon*" (2015) 20:1 Can Crim L Rev 93; Colton Fehr, "Cell Phone Searches Incident to Arrest: A Case Comment on the Ontario Court of Appeal's Decision in *R v Fearon*" (2014) 60:3 Crim LQ 343 [Fehr, "Cell Phone Searches"].

only a limited amount of scholarship has explored Canada's legislative ability to create laws governing digital devices.[15] These authors conclude that Parliament has risen to the challenge of governing privacy in the digital age.[16] Their conclusions, however, derive from Parliament's first few legislative responses to complex technological issues that arose from litigation under section 8 of the *Charter*.[17] As more difficult problems have arisen since these initial legislative reactions, more sustained study of parliamentary capacity to address the unique challenges of governing digital privacy is necessary.

As I conclude below, the initial academic optimism about Parliament's abilities in this regard was unwarranted. Parliament often passes digital privacy laws that are broad and indeterminate, leaving it to the courts to develop a framework for governing digital privacy intrusions. Where Parliament enacts laws tailored to address a narrow aspect of digital privacy, these laws often become stagnant, lead to incoherent results, or both. As courts are struggling to create informed rules within the adversarial framework, either legislatures must take a much more active role, or they must provide courts with better tools to decide issues relating to complex technologies. I contend that the latter approach is preferable since Parliament's institutional constraints will likely continue to prevent it from legislating quickly and coherently in response to the use of new and complex technologies. Instead, I maintain that courts and Parliament should work together to ensure judicial development of the law is expedient, coherent, and even-handed.

This article is divided into three parts. In Part I, I outline my methodology for exploring the institutional capacity of legislatures to govern digital privacy as opposed to courts. In Part II, I analyze Parliament's legislation governing complex and rapidly shifting technologies, asking whether this legislation responds quickly and coherently to technological change, and without undue influence. I conclude that Parliament suffers from many of the same weaknesses attributed to Congress in the American literature, although to varying degrees. Part III closes by using the article's findings to develop a normative framework for governing digital privacy. Contrary to much of the literature on institutional choice, I maintain that

---

15 Professor Steven Penney has addressed this question in "Reasonable Expectations", *supra* note 14 at 504–05 and in "Updating Canada's Communications Surveillance Laws: Privacy and Security in the Digital Age" (2008) 12:2 Can Crim L Rev 115 [Penney, "Updating Canada's Communications Surveillance Laws"]. See also Michal Fairburn, "Twenty-Five Years in Search of a Reasonable Approach" (2008) 40 SCLR (2d) 55.

16 *Cf* Fairburn, *supra* note 15 at 73, 75, 79–84.

17 See *ibid*; *Canadian Charter of Rights and Freedoms*, s 8, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11 [*Charter*].

Canadian courts should play a significant role with respect to governing digital technologies, at least in the context of criminal procedure.

I. Methodology

The term "digital technology" refers to electronic tools, systems, or devices that generate, store, or process data. Although my study primarily focuses on Parliament's legislative responses to digital technologies, other complex and rapidly developing technologies raise similar governance concerns and, therefore, are also appropriate objects of study.[18] As I explain in Part II, Parliament's legislative responses to these types of technologies have been enacted piecemeal over the last several decades. This time period provides ample opportunity to test parliamentary capacity to respond to digital privacy concerns.

In my review of the statutes, I seek to answer three main questions. First, I inquire as to whether Parliament has reacted quickly to developments in digital technologies. As noted above, this is one of the main weaknesses of allowing courts to create rules with respect to digital technologies. Judges operating within the adversarial system can only address technological issues when criminals or police have used new technologies in a legally relevant way.[19] Even after a technology is considered by a court, the appeals process will delay confirmation of any rule rendered at trial.[20] If Parliament reacts no more quickly than courts, this consideration will hold little sway in determining who is better capable of governing digital privacy.

Second, I will assess whether Parliament's responses have led to incoherent or unintended results. Again, this is a main critique of allowing courts to regulate digital technologies. Courts not only face time constraints when rendering decisions,[21] they are also limited to consideration

---

18 Parliament's first response to radio-based communication devices is one of several examples discussed in Part II, *below*.

19 See Scanlan, "Issues", *supra* note 6 at 312:

> When the subject of the decision is technology, the time between when the technology first appears, some criminal use is made of it, police investigations occur, trials are held, and appeals are heard can be many years. When dealing with a relatively stable technology like DNA analysis, no harm occurs. When the process occurs in relation to a specific digital technology or software, the result may well be an appellate pronouncement of historical interest only.

20 See *ibid*. See also Kerr, "Fourth Amendment", *supra* note 5 at 868–69.

21 See Kerr, "Fourth Amendment", *supra* note 5 at 875–76.

of the evidence submitted at trial.[22] Because adversarial proceedings tend to produce inadequate evidence of the operation of digital technologies, courts are prone to render decisions without vital information.[23] However, if Parliament is receiving inadequate evidence, conducting insufficient study, or passing laws in haste, it is likely that mistakes will also be found in its statutory scheme. If mistakes are made, its relative institutional competence will be undermined.

Finally, it is necessary to ask whether Parliament is subject to undue influence by special interest groups or ignores privacy interests to appeal to majoritarian bias. This is an important question in the context of search and seizure law, as prominent academics have questioned whether such concerns arise at all in the criminal law context.[24] Even if such concerns arise, others ask whether these concerns apply to novel search technologies, which are disproportionately owned by members of social classes that have few encounters with the criminal law.[25] If these concerns prove to be founded, and Parliament is unduly influenced, the value of judicial independence will assist courts in tailoring more balanced responses to governing digital privacy.

This inquiry is undertaken through the lens of public choice theory. Public choice theory applies microeconomics to political decision-making. Its broad contribution is to illustrate how the rational actor model applies to political actors.[26] Public choice theorists reject the assumption that political actors always act in the public interest, and seek to explain political behaviour by viewing political actors as "egoistic, rational, utility maximizer[s]."[27] Public choice theory is frequently used to explain inaction[28] and

---

22 See *ibid*. Although appellate courts sometimes receive intervener briefs, these briefs often fail to fill the informational lacuna. As Murphy, *supra* note 5 at 505–06 observes, this is likely because institutions that defend privacy, such as civil liberties associations, are not able to expend necessary resources due to their limited funding being divided between numerous civil rights issues.

23 See Kerr, "Fourth Amendment", *supra* note 5 at 875–76; Scanlan, "Issues", *supra* note 6 at 311–12.

24 See Kerr, "Fourth Amendment", *supra* note 5 at 885–87.

25 See *ibid*. See also Penney, "Reasonable Expectations", *supra* note 14 at 503–04.

26 See generally Daniel A Farber & Philip P Frickey, *Law and Public Choice: A Critical Introduction* (Chicago: University of Chicago Press, 1991).

27 See Dennis C Mueller, *Public Choice III* (Cambridge, UK: Cambridge University Press, 2003) at 1–2.

28 As Anthony Downs explains in *An Economic Theory of Democracy* (New York: Harper, 1957), the limited resources citizens possess to investigate complex political issues result in few issues defining an election. As a result, even extreme instances of privacy infringements (e.g., Snowden) have failed to significantly impact elections. Other more common privacy infringements—such as corporate collection and dissemination of data—rarely

anomalous action (often caused by lobbyist influence[29]) by legislatures. Applying this theoretical framework to complex search technologies will allow for a reasoned conclusion concerning why Parliament reacts in the manner it does with respect to said technologies.

Before embarking on this study, it is also prudent to explain what is *not* the subject of inquiry. First, I limit my study to federal criminal laws; including provincial legislation would make the study overly broad. As will become evident, Parliament's post-*Charter* criminal legislation includes sufficient case studies to shed general light on the normative capacity of Canadian legislatures to govern privacy, at least in the criminal law context. Second, my study excludes national security legislation. To investigate the speed, coherence, and public choice theory questions central to my study requires broad access to records related not only to the development of the laws, but also to how those laws are interpreted and acted upon. Generally speaking, such information is not sufficiently available. As one author aptly puts it, "[a]bsent whistle-blowers, it is almost impossible to develop enough understanding of the intelligence agencies and their practices to identify what should even be negatively framed in the first place."[30]

II. Parliament's Legislative Responses

To assess Parliament's ability to govern digital privacy, I have divided my analysis into three sections. The first considers whether Parliament responded quickly to a technology that arose in the jurisprudence or was widely used by the public. Whether the response was intelligible or had significant gaps will be the subject of the second inquiry. The third inquiry will assess whether public choice concerns have arisen when Parliament passes digital privacy laws. I offer institutional explanations for Parliament's successes and failures at each interval.

---

constitute more than a nuisance, again making these issues relatively unimportant. As such, it is arguably sensible that political actors would not race to provide privacy protections, since this is unlikely to result in increased votes. See also David R Mayhew, *Congress: The Electoral Connection* (New Haven: Yale University Press, 1974) at 125–27; Neil K Komesar, *Imperfect Alternatives: Choosing Institutions in Law, Economics, and Public Policy* (Chicago: University of Chicago Press, 1994) at 56.

29 See Murphy, *supra* note 5 at 504; Lawrence Lessig, *Code: Version 2.0* (New York: Basic Books, 2006) at 323.

30 Christopher Parsons, "Stuck on the Agenda: Drawing Lessons from the Stagnation of 'Lawful Access' Legislation in Canada" in Michael Geist, ed, *Law, Privacy and Surveillance in Canada in the Post-Snowden Era* (Ottawa: University of Ottawa Press, 2015) 257 at 273 [Parsons, "Stuck on the Agenda"]. See also Murphy, *supra* note 5 at 493.

A. Speed of Response

The adoption of the *Charter* resulted in a series of assertive decisions interpreting the scope of section 8, which protects against "unreasonable searches and seizures."[31] Perhaps unsurprisingly, Parliament's response was somewhat lagging in the first decade, as it also had to respond to a plethora of other *Charter* decisions. Despite the challenge of responding to the judicial interpretation of a new bill of rights, Parliament initially reacted relatively quickly to fill gaps in the law on several occasions. In later years, however, institutional limitations prevented timely, if any, legislative response.

1. Post-*Charter*

The passage of the *Protection of Privacy Act*[32] introduced what is now Part VI of the *Criminal Code*.[33] With this change, Parliament followed in the footsteps of its American counterpart and provided a comprehensive scheme for governing interceptions of private communications.[34] It defined "private communications" as "any oral communication, or any telecommunication, 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."[35] However, with the onset of communications technologies, the limitations of Part VI's ability to respond to privacy and law enforcement concerns were repeatedly exposed.[36]

One of the first challenges posed to the scope of Part VI arose from its application to analog pagers.[37] At least two courts concluded that these technologies did not attract a reasonable expectation of privacy, thereby precluding the need for an intercept warrant.[38] Two reasons formed the basis for this conclusion. First, it was possible that a third party would overhear the recorded messages when played back on the pagers' speakers.[39]

---

31 *Supra* note 17.

32 SC 1973-74, c 50.

33 RSC 1985, c C-46.

34 See *Wiretap Act*, 18 US Code §§ 2510–22 (1968).

35 *Criminal Code*, *supra* note 33, s 183.

36 See Penney, "Updating Canada's Communications Surveillance Laws", *supra* note 15 at 121.

37 See *ibid* at 122.

38 See *R v Nin* (1985), 34 CCC (3d) 89, [1985] JQ no 155 (CQ (Crim & Pen Div)) [*Nin*]; *R v Lubovac* (1989), 101 AR 119, 52 CCC (3d) 551 (ABCA), leave to appeal to SCC refused, 21678 (8 March 1990) [*Lubovac*].

39 See *Nin*, *supra* note 38 at 93; *Lubovac*, *supra* note 38 at 558.

Second, it was also possible for third-party pagers to access recorded messages by tuning into the same frequency as the receiving party's receiver.[40] Despite the fact that the volume of a speaker may be controlled, these courts refused to recognize a reasonable expectation of privacy in the devices.[41]

Similar difficulties arose from public use of cell phones.[42] Cell phones sent unencrypted analog signals that were available over publicly accessible radio waves, thereby giving rise to the question of whether they attracted a reasonable expectation of privacy.[43] In *R. v. Solomon*,[44] the court concluded that no reasonable expectation of privacy existed because the cell phone signals were publicly accessible. In *R. v. Cheung*,[45] however, a more detailed assessment of telephony was undertaken. In so doing, the court concluded that because of the many frequencies and transmission towers from which information is transferred over wireless networks used by some phones,[46] it would be rare to intercept any communications from these wireless phones.[47] As such, the user's expectation of privacy was held to be reasonable.[48]

In the late 1980s, a further issue arose with respect to whether the consent of one party to covertly record a conversation supplanted the other party's reasonable expectation of privacy. No legislative provision expressly permitted such activity. The police could therefore only rely on the evidence obtained if the accused's expectation of privacy was unreasonable.[49] As the consenting party could repeat the words in court, there was a basis to conclude that the accused gave up any reasonable expectation of

---

40 See *Lubovac*, *supra* note 38 at 558–59.

41 See Penney, "Updating Canada's Communications Surveillance Laws", *supra* note 15 at 122, citing Robert W Hubbard, Peter M Brauti, & Scott K Fenton, *Wiretapping and Other Electronic Surveillance: Law and Procedure* (Aurora, ON: Canada Law Book, 2002) at 6.5.3.

42 See Penney, "Updating Canada's Communications Surveillance Laws", *supra* note 15 at 122–23.

43 See *ibid*.

44 (1992), 77 CCC (3d) 264, [1992] JQ no 2371 (Qc Mun Ct).

45 (1995), 100 CCC (3d) 441, 1995 CarswellBC 627 (BCSC) [*Cheung*].

46 Differences in cellular technology will be discussed in Part II.B.1, *below*.

47 See *Cheung*, *supra* note 45 at paras 12–15.

48 See *ibid*.

49 It would not be a "search" for constitutional purposes. See *Hunter v Southam Inc*, [1984] 2 SCR 145 at 159, 11 DLR (4th) 641 [*Hunter*].

privacy.[50] In *R. v. Duarte*,[51] however, the Court rejected this argument. As Justice La Forest wrote, "[a] society which exposed us, at the whim of the state, to the risk of having a permanent electronic recording made of our words every time we opened our mouths might be superbly equipped to fight crime, but would be one in which privacy no longer had any meaning."[52] Given the "wholly unacceptable" danger to privacy brought on by such new technologies, the Court concluded that prior judicial authorization was required.[53]

Shortly after *Duarte*, the Court in *R. v. Wong*[54] considered whether Part VI applied to video recordings. As outlined above, Part VI only covered oral or voice communications when it was first enacted. It therefore did not apply to non-audio-equipped video recordings. A few years earlier, the Law Reform Commission of Canada had explicitly concluded that this gap in the legislation would not lead to "unjustifiable intrusion into privacy."[55] As a result, the police had taken advantage of this loophole and planted a non-audio-equipped video camera in the accused's hotel room. The Court ultimately found a breach of section 8, since the accused had a reasonable expectation of privacy in his hotel room.[56] As Part VI did not provide for a warrant power, it was again unable to serve legitimate law enforcement interests.

Around the same time *Duarte* and *Wong* were decided, the courts were also considering the legality of using digital number recorders to register the metadata relating to outgoing and incoming calls.[57] In *R. v. Fegan*,[58] the

---

50 This was in fact the conclusion of the United States Supreme Court in *Lopez v United States*, 373 US 427 (1963).

51 [1990] 1 SCR 30, 71 OR (2d) 575 [*Duarte* cited to SCR].

52 *Ibid* at 44.

53 See *ibid* at 45–46.

54 [1990] 3 SCR 36, 60 CCC (3d) 460 [*Wong*].

55 Law Reform Commission of Canada, "Electronic Surveillance" (1986) Department of Justice Canada Working Paper No 47 at 21.

56 See *ibid*.

57 The Quebec and Ontario Courts of Appeal have both described digital number recorders as follows:

> A digital number recorder (DNR) is activated when the subscriber's telephone is taken "off the hook." Electronic impulses emitted from the monitored telephone are recorded on a computer printout tape which discloses the telephone number dialled when an outgoing call is placed. The DNR does not record whether the receiving telephone was answered nor the fact or substance of the conversation, if any, which then ensues. When an incoming call is made to the monitored telephone, the DNR records only that the monitored telephone is "off the hook" when answered and the length of time during which the monitored telephone is in that position (see *R v Cody*, 2007 QCCA 1276 at para 11 [*Cody* CA]; *R v Fegan* (1993), 13 OR (3d) 88 at 96, 80 CCC (3d) 356 (ONCA) [*Fegan*]).

58 *Supra* note 57 at 98.

Ontario Court of Appeal found that no warrant was required to use digital number recorders because the service provider was not acting on behalf of the state. Had such activity occurred at the behest of the state, however, pre-authorization would have been required.[59] This conclusion derived from the then-recent decision in *R. v. Wise*,[60] wherein the Court considered whether police installation of a tracking device on a motor vehicle required prior judicial authorization. Even though the "beeper" device at issue was unsophisticated,[61] the Court found that its use breached the occupant's reasonable expectation of privacy. If such a minimal infringement required pre-authorization, then it was likely (contrary to an earlier appellate opinion[62]) that a digital number recorder would also require pre-authorization.[63] As the *Criminal Code* provided neither powers, such searches violated section 8 of the *Charter*.[64]

Parliament attended to many of these concerns in 1993 with Bill C-109.[65] To address the inapplicability of Part VI to wireless phone communications, Parliament amended the definition of "private communication" to include 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."[66] This ensured that some wireless telephone communications would require the state to meet the higher requirements for a Part VI intercept warrant.[67]

---

59 See *ibid*. See also *R v Griffith* (1988), 44 CCC (3d) 63 at 77, 5 WCB (2d) 208 (Ont Dist Crt); *R v Khiamal* (1990), 73 Alta LR (2d) 359, 106 AR 246 (ABQB).

60 [1992] 1 SCR 527, 70 CCC (3d) 193 [*Wise* cited to SCR].

61 See *ibid* at 534. The device was a low power radio transmitter that could provide a general location for the thing being tracked.

62 See *R v Samson* (1983), 45 Nfld & PEIR 132, 11 WCB 75 (Nfld CA).

63 See the last two paragraphs in *Fegan*, *supra* note 57 at 103.

64 For a search to be reasonable under section 8 of the *Charter*, it must be "authorized by law." See *R v Collins*, [1987] 1 SCR 265 at 278, 38 DLR (4th) 508 [*Collins*]. No law authorized the technique used in either *Fegan*, *supra* note 57 or *Wise*, *supra* note 60.

65 See Bill C-109, *An Act to Amend the Criminal Code, the Crown Liability and Proceedings Act and the Radiocommunication Act*, 3rd Sess, 34th Parl, 1993 (assented to 23 June 1993), SC 1993, c 40.

66 *Criminal Code*, *supra* note 33, s 183. See also Penney, "Updating Canada's Communications Surveillance Laws", *supra* note 15 at 123–24. Parliament also explicitly subjected wireless telecommunications to the wiretap warrant procedures. See *Criminal Code*, *supra* note 33, ss 184.5–184.6.

67 See Part II.B.1, *below*, for an explanation of why the amendments were not comprehensive.

Parliament's enactment of section 184.2 of the *Criminal Code* further provided for warrants to allow for consensual interception of communications. This addressed the concerns raised in *Duarte*. In addition, Parliament enacted provisions that permitted warrantless interception where bodily or imminent harm is reasonably foreseeable.[68] Although the requirements now found in section 184.2 do not provide the added protections of other Part VI warrants,[69] the courts have found the lower standard to be constitutional as the third-party privacy concerns raised by traditional intercepts are not engaged.[70] As Justice Watt observed in *R. v. Largie*,[71] "[p]articipant surveillance is generally more focused than third-party surveillance, targeting specific conversations with specific individuals."[72] Thus, not only do captures of third-party communications become less likely, but the state agent's control over the conversation also reduces the risk of accidentally receiving irrelevant but private information.[73]

To address the gap revealed in *Wong* regarding the non-applicability of Part VI to non-audio-equipped video recordings, Parliament enacted the general warrant provision under section 487.01. This broad provision offered a means for police to seek a warrant where no other legislative enactment prescribed a suitable power. It also specifically included sections 487.01(4) and (5), which extended Part VI to apply to any observation "by means of a television camera or other similar electronic device" of "any person who is engaged in activity in circumstances in which the person has a reasonable expectation of privacy."[74] Thus, Parliament not only provided police with a means to lawfully conduct non-audio-equipped video recordings, but also gave police a flexible tool to apply for search warrants where no specific *Criminal Code* provision applied.

Finally, in response to *Wise* and *Fegan*, Parliament enacted sections 492.1 and 492.2 of the *Criminal Code*. Section 492.1 allowed tracking warrants to be issued if the police had reasonable grounds to suspect an offence had been or would be committed and that information relevant to the offence could be obtained by using a tracking device. Section 492.2 allowed for the use of digital number recorders if police had reasonable grounds to suspect information related to an accused's telephone calls would aid in an

---

68 See *Criminal Code*, *supra* note 33, ss 184.1, 184.4.

69 Most notable is the absence of an investigative necessity requirement. For additional requirements, see *ibid*, s 487.01(5).

70 Constitutional challenges to section 184.2 have been unsuccessful. See *R v Bordage*, 146 CCC (3d) 549 at paras 14–44, [2000] JQ No 2045 (QCCA); *R v Largie*, 2010 ONCA 548 at paras 50–58, leave to appeal refused [2010] SCCA No 460.

71 *Supra* note 70.

72 *Ibid* at para 56.

73 See *ibid*.

74 *Criminal Code*, *supra* note 33, s 487.01(4).

investigation. This lower standard of reasonable suspicion was borrowed from the decision in *Wise*, wherein the Court concluded that any parliamentary response could allow for authorization on a lower standard given the lower privacy interests inherent in the information revealed by some searches.[75]

2. 1994–1997

The next parliamentary response to digital privacy concerns was less comprehensive, but no less important, as it updated the warrant powers for police officers under section 487 of the *Criminal Code*. This provision's scope extended only to "things" found in buildings, places, or receptacles. The problem raised by digital evidence was aptly summarized by Susan Magotiaux:

> Is a computer a thing? Is the data on it a thing? Is the string of binary code sent through satellites in pieces and reassembled at some other machine a thing? Is it the same "thing" when it lands as it is when it travels in pieces? And what of the places? Police can't knock and announce their presence at the door of satellites and clouds and mobile servers. Yet without particularity of place, current tools may be unavailable.[76]

To ensure police could seek warrants for digital "things," Parliament amended section 487 of the *Criminal Code* in 1997.[77] Subsections 487(2.1) and (2.2) were added to ensure police may apply to access and use computer systems found in the place of a search. These broad provisions provide that a police officer may "use or cause to be used any computer system at the building or place to search any data contained in or available to the computer system."[78]

3. 1998–2013

As computer technologies became more prevalent, the modes for committing a diverse amount of crimes were fundamentally transformed.[79] Unfortunately, the wording of many criminal offences did not capture acts

---

75 See *Wise*, *supra* note 60 at 556.

76 *Supra* note 14 at 510. See also James A Fontana & David Keeshan, *The Law of Search and Seizure in Canada*, 8th ed (Markham: LexisNexis, 2010) at 1181–82.

77 See Magotiaux, *supra* note 14 at 510.

78 *Ibid*.

79 See James A Fontana & David Keeshan, *The Law of Search and Seizure in Canada*, 9th ed (Toronto: LexisNexis, 2015) at 782 [Fontana & Keeshan, *Search and Seizure* 9th ed] (citing offences such as "fraud, money-laundering, distribution of child pornography, invasion of privacy, and production of counterfeit cheques, identification and bills of exchange," as well as other nefarious uses of computers).

committed with computer technologies, while other offences now prevalent in the digital age had not received any criminal prohibition. Parliament spent much of this period attempting to fill these legislative gaps.

The main area addressed by Parliament was broadly concerned with the sexual exploitation of minors. Digital technologies provided new and difficult-to-trace means of possessing and distributing child pornography.[80] The typical means of "possession" in the physical sense applied to those who downloaded child pornography.[81] However, determining whether accessing an image on an internet website constituted "possessing" the data posed conceptual difficulties.[82] Although evidence stored in the cache *may* provide sufficient evidence of knowledge and control, these core elements of possession will often be difficult to prove with such evidence.[83] Equally concerning, the definition of distributing child pornography did not extend to digital means of distribution, which had become increasingly common at the turn of the century.[84]

In response to these issues, Parliament enacted Bill C-15A in 2002.[85] This bill created the "accessing" child pornography offence now found in subsections 163.1(4.1) and (4.2) of the *Criminal Code*.[86] Parliament's purpose in making these arrangements was to "capture those who intentionally view child pornography on the net but where the legal notion of possession may be problematic."[87] Bill C-15A also amended the distribution of child pornography offence found in subsection 163.1(3) to include "transmission" and "making available" within the scope of the offence. This had the effect of ensuring that the "offence extends to distribution of child pornography in electronic form on the Internet by such means as e-mail and posting items to websites."[88] Parliament further passed section 164.1,

---

80 See *ibid* at 779.

81 See *R v Morelli*, 2010 SCC 8 at para 36 [*Morelli*].

82 See *ibid* at paras 34–37. See also *R v Weir*, 2001 ABCA 181 at paras 22–24 [*Weir*]; *R v Daniels*, 2004 NLCA 73 at paras 11–12; *R v Panko*, 2010 ONCA 660 at paras 57–72.

83 See *Morelli*, *supra* note 81 at paras 34–37.

84 See *ibid*.

85 Bill C-15A, *An Act to Amend the Criminal Code and to Amend Other Acts*, 1st Sess, 37th Parl, 2002 (assented to 4 June 2002), SC 2002, c 13.

86 See *ibid*, cl 5(3).

87 "Bill C-15, An Act to amend the Criminal Code and to amend other Acts", *House of Commons Debates*, 37-1, vol 137 No 54 (3 May 2001) at 3581.

88 Canada, Law and Government Division, *Bill C-15A: An Act to amend the Criminal Code and to amend other Acts* (Legislative Summary), by David Goetz & Gérald Lafrenière (Ottawa: Library of Parliament, 2001), online: <publications.gc.ca> [perma.cc/9R2U-7HWG].

which allowed for courts to order the removal and destruction of child pornography on the internet.[89]

Bill C-15A also introduced an offence for child luring by way of a "computer system."[90] The internet enabled the increased prevalence of this sort of predatory behaviour and, as such, the prohibition was tailored to combat the digital commission of these crimes.[91] Similarly, voyeurism offences had become increasingly prevalent with increased technological capacity. Parliament responded with a specific prohibition against recording people in private circumstances.[92] These and the child pornography provisions would not require any substantial amendments during this time period.

Parliament also updated several other offences to account for contemporary technology. For instance, the illegal gambling provisions in paragraph 202(1)(i) were amended in 2008 to include digital means for promoting or facilitating betting.[93] Section 342.01 was amended to include copying of "credit card data" as opposed to prohibiting only "forging or falsifying" credit cards, since the latter definition did not apply to the mere possession or use of a credit card's data.[94] Parliament also introduced a criminal prohibition for using recording technology (i.e., small cameras) to record private productions such as movies on display in a theatre.[95]

In addition to creating new or amending old criminal offences, Parliament passed its first production order scheme in 2004.[96] Production orders allow police to compel third parties who are not under investigation for any

---

89 See Bill C-15A, *supra* note 85, cl 7.

90 *Ibid*, s 8. "Telecommunication" is defined as an "emission, transmission or reception" of communicative content "by any wire, cable, radio, optical or other electromagnetic system, or by any similar technical system".

91 See *Criminal Code*, *supra* note 33, s 172.1.

92 See Bill C-2, *An Act to amend the Criminal Code (protection of children and other vulnerable persons) and the Canada Evidence Act*, 1st Sess, 38th Parl, 2005, cl 6 (assented to 20 July 2005), SC 2005, c 32 (which enacted the current section 162 prohibition).

93 See Bill C-13, *An Act to amend the Criminal Code (criminal procedure, language of the accused, sentencing and other amendments)*, 2nd Sess, 39th Parl, 2008, cl 5 (assented to 29 May 2008), SC 2008, c 18. The previous version of the offence applied only to "radio, telegraph, telephone, mail or express" forms of information transmission. Section 204(2) was amended to address a similar gap (*ibid,* cl 6).

94 See Bill S-4, *An Act to amend the Criminal Code (identity theft and related misconduct)*, 2nd Sess, 40th Parl, 2009, cl 5 (assented to 22 October 2009), SC 2009, c 28.

95 See Bill C-59, *An Act to amend the Criminal Code (unauthorized recording of a movie)*, 1st Sess, 39th Parl, 2007, cl 1 (assented to 22 June 2007), SC 2007, c 28. The offence now exists under *Criminal Code*, *supra* note 33, s 432.

96 See Bill C-13, *An Act to amend the Criminal Code (capital markets fraud and evidence-gathering)*, 3rd Sess, 37th Parl, 2004, cl 7 (assented to 29 March 2004), SC 2004, c 3.

offence to produce data or documents that may be relevant to the commission of an offence by another person.[97] The impetus to pass this scheme arose from Canada's 2001 signing of the Council of Europe's *Convention on Cybercrime*.[98] The convention requires that all signatories criminalize certain offences commonly committed on computers and improve investigative techniques for detecting online crime. By adopting this framework, the signatories aimed to facilitate increased co-operation between countries investigating cybercrime.[99]

Parliament's legislation furthered these goals by providing police with two types of production orders: a general production order issuable on reasonable grounds to believe an offence occurred and a specific order relating to financial or commercial data issuable on reasonable suspicion.[100] Subsequent attempts in 2005,[101] 2009,[102] 2010,[103] and 2012[104] to bring in more narrowly tailored production orders, as well as provide a variety of other police powers necessary to ratify the *Cybercrime Convention*,[105] were un-

---

97 See Fontana & Keeshan, *Search and Seizure* 9th ed, *supra* note 79 at 494.

98 See Council of Europe Treaty Office, "Details of Treaty No 185: Convention on Cybercrime" (last visited 5 March 2019), online: <conventions.coe.int> [perma.cc/XGM8-8K66] [Details of Treaty No 185]. Canada signed on 23 November 2001: see Council of Europe, "Chart of Signatures and Ratifications of Treaty 185: Convention on Cybercrime" (last visited 9 March 2019), online: <www.coe.int> [perma.cc/D9ZV-K7GX].

99 See Details of Treaty No 185, *supra* note 98.

100 See *Criminal Code*, *supra* note 33, ss 487.014–017. For the difference between the two standards, see *R v Chehil*, 2013 SCC 49 at para 27 [*Chehil*] ("while reasonable grounds to suspect and reasonable and probable grounds to believe are similar in that they both must be grounded in objective facts, reasonable suspicion is a lower standard, as it engages the reasonable possibility, rather than probability, of crime").

101 See Bill C-74, *An Act regulating telecommunications facilities to facilitate the lawful interception of information transmitted by means of those facilities and respecting the provision of telecommunications subscriber information*, 1st Sess, 38th Parl, 2005 (first reading 15 November 2005).

102 See Bill C-46, *An Act to amend the Criminal Code, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act*, 2nd Sess, 40th Parl, 2009 (first reading 18 June 2009); Bill C-47, *An Act regulating telecommunications facilities to support investigations*, 2nd Sess, 40th Parl, 2009 (first reading 18 June 2009).

103 See Bill C-50, *An Act to amend the Criminal Code (interception of private communications and related warrants and orders)*, 3rd Sess, 40th Parl, 2010 (first reading 29 October 2010); Bill C-51, *An Act to amend the Criminal Code, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act*, 3rd Sess, 40th Parl, 2010 (first reading 1 November 2010); Bill C-52, *An Act regulating telecommunications facilities to support investigations*, 3rd Sess, 40th Parl, 2010 (first reading 1 November 2010).

104 See Bill C-30, *An Act to enact the Investigating and Preventing Criminal Electronic Communications Act and to amend the Criminal Code and other Acts*, 1st Sess, 41st Parl, 2012 (second reading 14 February 2012).

105 See Details of Treaty No 185, *supra* note 98. The police powers passed by Parliament discussed in the next subsection were required to ratify the Convention.

successful. Either the Conservative government received limited opposition party support when in a minority position, an election was called causing the proposals to die on the order table, or, as discussed in detail below,[106] public backlash caused government to retract its proposal.[107]

4. 2014–Present

The advent of email and text messaging introduced novel challenges for Part VI intercepts. Under section 183, the meaning of "intercept" includes to "listen to, record or acquire a communication or acquire the substance, meaning or purport thereof."[108] Courts and academics had long argued that inclusion of the word "acquire" made it necessary to apply for a Part VI warrant to access retrospective email and text messages.[109] Others, however, concluded that the plain meaning of "intercept" required that the acquisition of the message occur during its transmission.[110] As this distinction fundamentally alters the prerequisites for obtaining private communications,[111] several courts heard arguments with respect to when a state act qualified as an "intercept."[112]

---

106 See Part II.C, *below*.

107 See Parsons, "Stuck on the Agenda", *supra* note 30 at 261–63.

108 See *Criminal Code*, *supra* note 33, s 183.

109 See e.g. Charles Morgan, "Employer Monitoring of Employee Electronic Mail and Internet Use" (1999) 44:4 McGill LJ 849 at 875; Steve Coughlan, "*Telus*: Asking the Right Questions About General Warrants" (2013) 100 CR (6th) 290; Alan D Gold, "'If the Shoe Fits... and Wonderfully So': Part VI of the *Criminal Code* Should Be Applied to Digital Communications" (2016) 28 CR (7th) 44; Gerald Chan, "What Does *Telus* Say About Retrospective Seizures of Private Communications?", *For the Defence* 34:4 (28 October 2013). See also Jarrod J White, "E-Mail@Work.Com: Employer Monitoring of Employee E-Mail" (1997) 48:3 Ala L Rev 1079 at 1083; Tatsuya Akamine, "Proposal for a Fair Statutory Interpretation: E-Mail Stored in a Service Provider Computer Is Subject to an Interception Under the Federal Wiretap Act" (1999) 7:2 JL & Pol'y 519 at 561–65. It is notable that Justice Abella left this question open in *R v Telus*, 2013 SCC 16 at para 15 [*Telus*]. Post-*Telus* only one court agreed with this interpretation. See *R v Croft*, 2013 ABQB 640 at para 43 [*Croft*].

110 See e.g. Penney, "Updating Canada's Communications Surveillance Laws", *supra* note 15 at 127, citing *Weir*, *supra* note 82 and *R v McQueen* (1975), 25 CCC (2d) 262 at 265, 1975 CarswellAlta 79 (ABCA). For post-*Telus* cases rejecting this definition of "acquire" see *R v Belcourt*, 2015 BCCA 126 at para 55; *R v Webster*, 2015 BCCA 286 at paras 62–63; *R v Carty*, 2014 ONSC 212 at para 63; *R v Didechko*, 2015 ABQB 642 at paras 302–03; *R v Pazder*, 2015 ABQB 493 at paras 117–18.

111 If the police seek to intercept a private communication, they must meet numerous requirements that are much more restrictive than those required under the general warrant or the production order provisions. See generally *Criminal Code*, *supra* note 33, ss 185–96.

112 See *supra* notes 109–10.

The Supreme Court of Canada partially addressed this issue in *Telus*.[113] Unlike other telecommunications providers, Telus stores all messages sent through its infrastructure on a computer database for thirty days.[114] The police wanted to retrieve historical messages from this database, as well as future messages throughout the course of a warrant.[115] Rather than applying for a production order and an intercept warrant, the police applied for a general warrant under section 487.01.[116] A plurality of the Court found the acquisition of the future messages to be an "intercept," since any *prospective* capture of communications engages the purpose of Part VI.[117] The remaining members of the majority concluded that this technique was "substantively equivalent" to an intercept.[118] The dissent found that Part VI drew a distinction between *interception* and *use*, *retention*, *or disclosure* of a communication.[119] As Telus was disclosing to police what it had independently intercepted during its delivery process, the practice did not qualify as an "intercept."

The issue of whether an intercept warrant was required for purely historical emails or text messages reached the Court four years later in *R. v. Jones*.[120] The Court adopted the dissenting view in *Telus* that the statutory scheme supported the distinction between disclosure and interception. As such, police need only apply for a production order to obtain historical messages. Although this issue is now settled (barring a constitutional challenge),[121] it is notable that Parliament failed to update its legislation despite these ambiguities being known to the federal government for well over a decade.[122]

The use of peer-to-peer file sharing networks in the context of child pornography investigations also posed difficulties for police investigations. These networks allow users to download files directly from another user's

---

113 *Supra* note 109.

114 See *ibid* at paras 7, 58. It does so to aid in troubleshooting problems.

115 See *ibid* at para 9.

116 See *ibid* at para 8. As no single warrant power allowed the police technique at issue, the Crown argued that a general warrant was available.

117 See *ibid* at para 42.

118 See *ibid* at paras 52–53. They did not attempt to refine the definition of "intercept" because of the inherently complex nature of digital technologies and the need to "[guard] against unforeseen and potentially far-reaching consequences."

119 See *ibid* at paras 137, 143–44. See also *R v Jones*, 2017 SCC 60 at paras 59–74 [*Jones*].

120 *Supra* note 119.

121 See Justice Rowe's reasons in *Jones*, *supra* note 119 at paras 83–87. I discuss the merits of this challenge in Part II.B, *below*.

122 See Canada, Parliamentary Information and Research Service, *Legislative Summary of Bill C-74: Modernization of Investigative Techniques Act*, by Dominique Valiquet (Ottawa: Library of Parliament, 2005) at D(5), online: <lop.parl.ca> [perma.cc/MNJ5-LJ4X] [*Legislative Summary of Bill C-74*].

computer. As users are anonymous online, police must begin such investigations by procuring the Internet Protocol (IP) address that obtained the child pornography files.[123] The investigating officer can then run the IP address through a database that matches IP addresses with approximate locations and service providers.[124] The officer then makes a "law enforcement request" to the relevant service providers requesting that it release the subscriber information related to the IP address.[125] With this information, the police may then obtain a warrant to seize and search the suspect's computer.[126]

These were the facts underlying the Court's decision in *R. v. Spencer*,[127] as well as a series of earlier lower court decisions dating back to the mid-2000s.[128] The accused in *Spencer* successfully argued that he had a reasonable expectation of privacy in his subscriber information.[129] As such, the Court concluded that state requests for Internet Service Provider (ISP) subscriber information qualify as a search under section 8 of the *Charter*, thereby requiring lawful authority to conduct the search. As there was no suitable provision authorizing the state to make such requests,[130] the search was found to be unconstitutional.[131]

Technological change also affected the intrusiveness of tracking warrants. Tracking warrants are frequently attached to objects, such as vehicles, but now are also available to monitor mobile devices frequently carried on the person. The ability to track a person's precise location with Global Positioning System (GPS) technology, as opposed to the unsophisticated methods at issue in *Wise*, poses significantly more serious threats to privacy. As such, it was questionable whether tracking a person based on

---

123 See Colton Fehr, "A Proposal for Police Acquisition of ISP Subscriber Information on Administrative Demand in Child Pornography Investigations" (2019) 24:2 Can Crim L Rev 235 [Fehr, "Proposal"]; *Spencer*, *supra* note 4 at para 8.

124 See Fehr, "Proposal", *supra* note 123.

125 See *ibid*.

126 See e.g. *Spencer*, *supra* note 4 at paras 12–13.

127 *Ibid*.

128 See e.g. *R v Ward*, 2008 ONCJ 355, aff'd 2012 ONCA 660; *R v Vasic*, [2009] OJ No 685, 185 CRR (2d) 286; *R v Trapp*, 2011 SKCA 143; *R v Trapp*, 2009 SKPC 109; *R v Friers*, 2009 ONCJ 103; *R v Wilson*, [2009] OJ No 1067, 2009 CarswellOnt 2064; *Re SC*, 2006 ONCJ 343; *R v Kwok*, [2008] OJ No 2414, 78 WCB (2d) 21; *R v Cuttell*, 2009 ONCJ 471.

129 See *Spencer*, *supra* note 4 at para 51.

130 See *ibid* at paras 63–65. Section 7(3)(c.1)(ii) of the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 [*PIPEDA*], requires that the state actor identify its "lawful authority" for making the request. The police were, however, relying on this section as *the* authority for the request. This reasoning was rightly found to be circular.

131 See *Spencer*, *supra* note 4 at paras 68–74.

"reasonable suspicion" still struck an appropriate balance between privacy and law enforcement interests.[132]

The utility of digital number recorders was also impacted by technological developments. Section 492.2 of the *Criminal Code* originally stipulated that a "number recorder" was "any device that could be used to record or identify the telephone number or location of the telephone from which a telephone call originates, or at which it is received or is intended to be received."[133] As people now frequently communicate with other media such as email and text, it was necessary to create a broader framework for capturing metadata with respect to such communications. It was also unclear if the retrievable data under section 492.2 included the place at which the call was made and received. Arguably this would also be constitutional, but the legislation needed to explicitly allow for such a search.[134]

Finally, the Court was presented with the issue of whether searching cell phones incident to arrest was constitutional.[135] This issue has especially important implications for digital privacy.[136] As such, the Court's decision to allow warrantless cell phone searches incident to arrest—when many cell phones are functionally equivalent to computers[137]—was controversial. For a variety of reasons, the Court's ruling has been heavily criticized.[138] Anticipating its institutional shortcomings to develop a comprehensive rule, the majority invited Parliament to pass legislation governing when police may conduct such searches.[139]

---

[132] See *R v Grandison*, 2016 BCSC 1712 [*Grandison*]; *R v Brown*, 2014 ONSC 6323.

[133] *Criminal Code*, *supra* note 33, s 492.2.

[134] See Penney, "Updating Canada's Communications Surveillance Laws", *supra* note 15 at 150–51.

[135] See *R v Fearon*, 2014 SCC 77 [*Fearon*].

[136] See e.g. Don Stuart, *Charter Justice in Canadian Criminal Law*, 6th ed (Toronto: Carswell, 2014) at 283, citing American Law Institute, *Model Code of Pre-Arraignment Procedure* (Philadelphia: The Institute, 1975) at 493–94 (highlighting that in the United States, searches incident to arrest occur approximately forty times more often than warranted searches).

[137] See *Fearon*, *supra* note 135 at para 54.

[138] See Steven Penney, "Searches of Digital Devices Incident to Arrest: *R v Fearon*" (2014) 23:2 Const Forum Const 1; Steven Penney, "Fear the Fearon? Searches of Digital Devices Incident to Arrest" (6 February 2015), online (webcast): *YouTube* <youtu.be/9hSN3MpxM7M>; Tim Quigley, "*R. v. Fearon*: A Problematic Decision" (2015) 15 CR (7th) 281; Fehr, "Cell Phone Searches", *supra* note 14; Fehr & Biden, *supra* note 14; Daniel M Scanlan, *Digital Evidence in Criminal Law* (Aurora, ON: Canada Law Book, 2011) at 214 [Scanlan, *Digital Evidence*], citing *R v Beauchamp* (2008), 58 CR (6th) 177 at paras 18, 66, 171 CRR (2d) 358 (Ont Sup Ct); Fine, *supra* note 14; Graham Mayeda, "My Neighbour's Kid Just Bought a Drone... New Paradigms for Privacy Law in Canada" (2015) 35 NJCL 59 at 79–81.

[139] See *Fearon*, *supra* note 135 at para 84.

Parliament addressed some of these concerns in 2014 with Bill C-13.[140] To address the gap in *Spencer*, as well as other more general gaps in the production and preservation order scheme, Parliament overhauled sections 487.011 to 487.0199 of the *Criminal Code*. Three main production orders were created, all issuable upon reasonable grounds to suspect an offence has been or will be committed. Sections 487.015 and 487.016 were added to allow police to trace and have third parties produce "transmission data."[141] Transmission data is effectively metadata—that is, the contextual information surrounding a communication.[142] Acquiring such data allows police to trace the origin of any telecommunication.[143] Section 487.017 allows police to apply for "tracking data," being data that "relates to the location of a transaction, individual or thing."[144] The amendments also provided police with the ability to compel third parties to preserve documents in their possession for a prescribed period. As such information is routinely destroyed (sometimes intentionally but often inadvertently), this provision was necessary to preserve evidence for crimes committed with digital technologies.[145]

Parliament further responded to concern over the constitutionality of tracking device warrants available under section 492.1 of the *Criminal Code* by raising the standard from reasonable suspicion to reasonable grounds to believe when the device being tracked is commonly on the person.[146] Parliament simultaneously updated the digital number recorder provision to include the broader term "transmission data."[147] This allowed police to obtain data indicating the origin and intended recipient of internet

---

140 See Bill C-13, *An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act*, 2nd Sess, 41st Parl, 2014 (assented to 9 December 2014), SC 2014, c 31.

141 *Ibid*, cl 20.

142 Such "data about data" includes the time and duration of a communication, the device used, its number, the numbers it called, and its location.

143 See Canada, Parliamentary Information and Research Service: Legal and Social Affairs Division, *Bill C-13: An Act to Amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act* (Legislative Summary), by Julia Nicol & Dominique Valiquet, Publication No 41-2-C13-E (Ottawa, Library of Parliament, 2013) at 2.1.12, online: <lop.parl.ca> [perma.cc/Q6GM-LRQX] [Legislative Summary of Bill C-13].

144 See *Criminal Code*, *supra* note 33, s 487.011.

145 See Legislative Summary of Bill C-13, *supra* note 143 at 2.1.11. For instance, telecommunications companies frequently destroy communications information after a prescribed period.

146 See Bill C-13, *supra* note 140, s 492.1(1). See also *Chehil*, *supra* note 100 at para 27 (explaining the distinction between "reasonable suspicion" and "reasonable grounds to believe").

147 Defined in *Criminal Code*, *supra* note 33, s 492.2(6).

and text communications, not just telephone communications.[148] The revised definition also clarified that location data during the transmission of a call may be obtained, a question left open by the previous provisions.[149] The fact that it took until 2014 to update these provisions, however, is evidence of Parliament's difficulty keeping pace with digital technologies.

Finally, Bill C-13 updated the *Criminal Code* by providing an offence for what has come to be known as "cyberbullying."[150] A legislative gap arose because digital technologies made it easy for young persons to distribute sexually explicit photos of their peers. Because charging youth with distribution of child pornography was too harsh a sanction,[151] Parliament introduced subsection 162.1(1) of the *Criminal Code*. Although the section in many ways mirrored the existing child pornography offences, it provided prosecutors with more moderate sentencing options for prosecuting youth and young adults than the child pornography provisions.[152]

5. Summary

Several conclusions may be drawn from the above review. Parliament's first few responses to gaps or constitutional issues with its legislative framework governing complex technologies were relatively quick.[153] At the turn of the century, however, Parliament became much less efficient. Despite having undertaken to provide a comprehensive lawful access scheme with its signing of the *Convention on Cybercrime* in 2001,[154] Parliament's legislation was patchwork and slow. Parliament did, however, manage to meet the requirements of the convention fourteen years after it was

---

148 See Fontana & Keeshan, *Search and Seizure* 9th ed, *supra* note 79 at 563.

149 See Penney, "Updating Canada's Communications Surveillance Laws", *supra* note 15 at 149. The new section contains a broad reference to the "origin" of any transmission data (see *Criminal Code*, *supra* note 33, s 492.2(6)).

150 This term refers to "the use of information and communication technologies to support deliberate, repeated and hostile behaviour by an individual or group that is intended to harm others." The term was coined in Bill Belsey, "Cyberbullying: A Real and Growing Threat", *ATA Magazine* 88:1 (Fall 2007) 14 at 15.

151 See *Criminal Code*, *supra* note 33, s 163.1(3) (prescribing a mandatory minimum penalty of one-year imprisonment).

152 See Legislative Summary of Bill C-13, *supra* note 143 at 2.1.2.1.1. It is also notable that the *Criminal Code*, *supra* note 33, s 164.1(1) provides for a warrant of seizure for such material to prevent further distribution on the internet.

153 Parliament's initial response received some judicial praise. See *R v Backhouse* (2005), 194 CCC (3d) 1 at para 110, 28 CR (6th) 31 (Ont CA) (per Justice Rosenberg, "Parliament has moved quickly to fill in gaps in the legislative scheme of search and seizure to provide the police with the necessary tools to investigate crime while ensuring that the public and individual interests in privacy are adequately protected").

154 "Lawful access" refers to state expansion of its capacity to collect communications data and subscriber information. See Part II.C, *below*.

adopted.[155] In the interim, the Crown pursued drawn-out litigation in the courts trying to find lawful access provisions where none existed.[156] Disputes surrounding Part VI warrants fared no better, as Parliament's refusal or inability to address the confusion surrounding the definition of "private communication" and "intercept" was ultimately left to the courts.[157] Although the digital number recorder warrant was eventually updated, the provision was inapplicable to many of the most common mediums of communication for two decades. Other issues with significant digital privacy implications, such as searches of cell phones incident to arrest or guidelines for searching computers under subsections 487(2.1) and (2.2), have so far received no response from Parliament.[158]

Parliament did fare better in defining offences—a domain where it could not rely on courts to fill in legislative gaps. Several offences were modified in the early- to mid-2000s to allow prosecution of new ways of committing crime brought on by digital technologies. Parliament's record with respect to updating offences, however, is not perfect. As Peter McKay observed, given the seriousness of the child pornography offence, the delay in updating these provisions was "virtually inexcusable."[159] The well-known practice of cyberbullying had also been an issue long before Parliament's legislation passed. More than anything, the response was a reaction to high profile teenage suicides.[160] Moreover, other desirable offences—such as a criminal prohibition for accessing and stealing historical data—have

---

155 See Foreign Affairs, Trade and Development Canada, "Canada Completes Ratification of Convention on Cybercrime" (8 July 2015), online: *Government of Canada* <www.canada.ca> [perma.cc/K59L-YR42].

156 See *Spencer*, *supra* note 4 and its discussion of section 7(3) of *PIPEDA*, *supra* note 130 at 68–74.

157 See e.g. *Telus*, *supra* note 109; *Jones*, *supra* note 119.

158 It is notable that some authors believe that the reason there was less legislation from Parliament was because of the Court's proactive approach to governing privacy. See Steven Penney, Vincenzo Rondinelli & James Stribopoulos, *Criminal Procedure in Canada*, 2nd ed (Toronto: LexisNexis, 2018) at 224–25. Although this is true with other privacy laws, I see little evidence of this in the context of governing complex and rapidly shifting search technologies.

159 See "Bill C-15, An Act to amend the Criminal Code and to amend other Acts", *House of Commons Debates*, 37-1, vol 137 No 097 (18 October 2001) at 6331.

160 The suicides of Rehtaeh Parsons and Amanda Todd were often cited in legislative debate and public discourse.

still not received criminal sanction.[161] Overall, although Parliament has responded reasonably quickly when updating offences, its record has blemishes.[162]

Any attempt at explaining Parliament's slow response time will, to some extent, be guesswork. However, it is not unreasonable to at least partially explain significant delays by observing that Canadian governments are often in a minority position. This was the case from 2004 to 2011, a period where legislative amendments regarding controversial privacy issues such as "lawful access" were repeatedly stifled.[163] A great deal more legislation was passed in the following years, which witnessed a Conservative majority government. It is also important to note, however, that all opposition parties during the Conservative government's time in power cited instances where the cause of delay was the Conservative government's tendency to shelve bills containing criminal justice issues, and then re-raise the bills to distract from scandals or to drum up political support around election time.[164] The "tough on crime" angle suggests that majoritarian politics were at play, and that the government was willing to sacrifice privacy interests for political gain.

B. Coherence of Response

The coherence of Parliament's responses to complex and rapidly advancing search technologies is equally illustrative of its relative institutional capacity to govern digital privacy. As will be seen, both privacy advocates and law enforcement have expressed concern about significant deficiencies with Parliament's legislative responses. Many of the technological developments were not anticipated by Parliament. Other anomalous results arose from unclear legislative drafting, which may be attributed to a failure to fully comprehend digital technologies. Still other responses relied on highly questionable determinations that the technology at issue did not attract a reasonable expectation of privacy.

---

[161] As Penney explains, traditional crimes such as theft and mischief do not catch this conduct (see "Updating Canada's Communications Surveillance Laws", *supra* note 15 at 137–43). Moreover, given the low likelihood of getting caught and sued, it is unlikely that this activity will be deterred. As such, it is necessary for the stigma of criminal conviction to raise deterrence to a sufficient level.

[162] This was found to result in an inability to bring charges in several cases. See "Bill C-46, An Act to amend the Criminal Code, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act", *House of Commons Debates,* 40-2, vol 144 No 100 (26 October 2009) at 6192 [Bill C-46, Debate].

[163] See *supra* notes 100–03. I will discuss the lawful access experience in detail in Part II.C, *below*.

[164] See e.g. "Bill C-47, An Act regulating telecommunications facilities to support investigations", *House of Commons Debates*, 40-2, vol 144 No 101 (27 October 2009) at 6247, 6250–51 [Bill C-47, Debate].

1. Wireless Phones

Parliament's 1993 amendment to the definition of "private communication" ensured that all encrypted digital signals sent via wireless phones came within the ambit of the term.[165] However, the various technologies used by different "generations" of cordless phones resulted in many then-current technologies falling outside of the amended definition of private communication. First generation cordless phones, which at the time of the amendments were used by 95 per cent of telephone users,[166] were susceptible to interception by simple scanner devices.[167] As a result, some courts held that communications via these phones did not attract a reasonable expectation of privacy.[168] These phones, like their analog pager predecessors, could therefore be tapped by anyone, including police, at will.

Other courts, in line with modern jurisprudence on section 8 of the *Charter*, concluded that the technical capabilities of private communication technology and their ability to be intercepted should not be the only factor considered.[169] To exclude 95 per cent of then-current cordless phone users was arguably not in line with what the average consumer would expect, as it is unlikely that anyone other than the police was frequently trying to intercept phone calls.[170] Moreover, placing emphasis on the type of phone one owns allows those who can afford to purchase newly available technologies to have greater privacy protections.[171] Parliament, then, arguably

---

165 See Bill C-109, *supra* note 65.

166 See *R v Penna* (1997), 36 WCB (2d) 483 at para 13, [1997] BCJ No 3014 (BCSC) [*Penna*].

167 See *ibid*. See also *R v Watts*, 2000 BCPC 191 at paras 6–12 [*Watts*]. Second generation phones send encrypted signals, making interception of a communication generally unintelligible. Third generation phones, in addition to sending encrypted messages, also frequently change the frequency with which the signal was sent making it extremely unlikely that the message could be intercepted, let alone made intelligible.

168 See *Penna*, *supra* note 166 at paras 13–18; *Watts*, *supra* note 167 at paras 8, 12 (though note that the judge came to this conclusion "reluctantly").

169 See *Watts*, *supra* note 167 at paras 8, 11. The Court in *Fearon* concluded that distinguishing between the capacities of dumb and smart phones was ill advised when developing the legal framework for searching cell phones incident to arrest (see *supra* note 134 at paras 52, 161). See also *Telus*, *supra* note 109 at para 5 ("[t]echnical differences inherent in new technology should not determine the scope of protection afforded to private communications").

170 See *Watts*, *supra* note 167.

171 As Member Derek Lee observed, "[a]pparently the only people ... who are protected under the new bill [C-109] ... are the ministers of the government, all of whom have encrypted conversation facilities. Government ministers are protected under the bill but ordinary Canadians are not." See "Bill C-109, An Act to amend the Criminal Code, the Crown Liability and Proceedings Act and the Radiocommunication Act", *House of Commons Debates*, 34-3, vol 14 (30 April 1993) at 18768.

drew an arbitrary and unfair distinction in its first amendment to the definition of private communication.

2. Tracking Device Warrants

In its 2014 amendments, Parliament elevated the grounds necessary for issuance of a tracking device warrant if the device is commonly found on the person. Given the onset of GPS tracking, this sounds like a principled approach. However, this approach may unduly limit police, depending on what technique is used to track a device. Tracking a cell phone, for instance, may involve police using a tactic known as "pinging." This practice indicates to police the cell phone tower with which a cell phone is exchanging signals. In *Grandison*, the expert testimony revealed that the information gained from this tactic told police that the accused was anywhere from a 50- to 4,894-metre radius from a tower.[172] The court also noted that pinging does not involve constant tracking of the subject, but instead requires that police make specific requests to the telecommunication service provider to determine the subject's approximate location at any given time.[173] This is contrary to GPS tracking, wherein an accused's exact location can be determined at any time.[174]

With a fuller understanding of the technology used for tracking the accused's phone, the court rejected the accused's contention that using the previous reasonable grounds to suspect standard was unconstitutional.[175] It came to this conclusion despite the amendments raising the relevant burden of proof having been implemented between the time the charge arose and when the court rendered its decision. Although the technique at issue was somewhat more sophisticated than the vehicle tracker used in *Wise*, the court concluded that the information revealed did not, unlike the use of GPS technologies, significantly touch on the biographical core of personal information required to constitutionally impose the higher reasonable and probable grounds standard.[176] Parliament's amendment, although well intended, therefore inadvertently prevented police from using other reasonable and less invasive methods of cell phone tracking.

---

[172] See *Grandison*, *supra* note 132 at paras 64–65.

[173] See *ibid* at para 66.

[174] See *ibid* at paras 68–69. For an example where the state employed GPS technology under section 492.1 of the *Criminal Code*, *supra* note 33, see *R v T & T Fisheries*, [2005] PEIJ No 74 at para 5, 2005 CarswellPEI 71 (PEI Prov Ct).

[175] See *Grandison*, *supra* note 132 at para 74.

[176] See *ibid* at para 73.

3. Digital Number and Transmission Data Recorders

As noted in the preceding section, the initial language of section 492.2 ("digital number recorder") was not broad enough to encompass metadata relating to technologies other than telephone calls. This had the effect of leaving metadata related to technologies such as email and text to be sought under the general warrant or production order provisions.[177] As these provisions require reasonable grounds to believe, they raised the standard for receiving what is effectively the same information from the lower reasonable suspicion standard required under section 492.2.[178] This was undesirable from a law enforcement perspective, since metadata is often used early on to further an investigation and therefore is needed *to make out* reasonable and probable grounds for a warrant.[179] Although the 2014 amendments corrected this mistake, it had persisted in the *Criminal Code* for twenty-one years.

4. General Warrants

Parliament enacted the general warrant provision found in section 487.01 to allow courts to issue warrants authorizing police to "use any device or investigative technique or procedure or do any thing described in the warrant that would, if not authorized, constitute an unreasonable search or seizure."[180] Although section 487.01 provides police with a flexible law enforcement tool,[181] it must be acknowledged that it abdicates authority for governing many novel search technologies to the courts. For in-

---

177 See Penney, "Updating Canada's Communications Surveillance Laws", *supra* note 15 at 144.

178 It is notable that use of the reasonable suspicion standard has generally withstood constitutional challenge. See *R v Cody*, [2004] QJ No 14164 at para 21, 2004 CanLII 50574 (Qc Sup Ct), aff'd in *Cody* CA, *supra* note 57; *Croft*, *supra* note 109 at paras 11–13; *Grandison*, *supra* note 132 at paras 126–27, all refusing to follow two lower court decisions that earlier decided reasonable suspicion was not a suitable standard for such searches. See *R v Nguyen*, 2004 BCSC 76 at para 30; *R v Hackert*, [1997] OJ No 6384 (Ont Ct J), aff'd [2000] OJ No 3495, 2000 CanLII 16866 (ONCA). The contention that use of a dial number recorder qualified as a Part VI intercept has also failed. See *Fegan*, *supra* note 57 at 103. The term "intercept" contemplates communication *content* being exchanged.

179 See Penney, "Updating Canada's Communications Surveillance Laws", *supra* note 15 at 146–47.

180 *Criminal Code*, *supra* note 33, s 487.01(1).

181 The idea of allowing courts to issue warrants for police tactics that Parliament had not contemplated has received significant criticism. See Steven Coughlan, *Criminal Procedure*, 2nd ed (Toronto: Irwin Law, 2012) at 133–34. However, constitutional challenges to the provision have been rejected. See *R v Lucas*, 2014 ONCA 561 at paras 104–26, leave to appeal to SCC refused, 35976 (22 January 2015) [*Lucas*]; *R v Kuitenen*, 2001 BCSC 677 [*Kuitenen*].

stance, the following investigative techniques have all been governed under section 487.01: Forward Looking Infrared (FLIR) thermal imaging,[182] installation of "amp meters" to measure electricity usage,[183] making electronic copies of data on a computer system,[184] review of third-party forensic files,[185] the ability to program failures into a criminal suspect's computer hardware,[186] use of forensic fluorescent light technologies to covertly search for bloodstains,[187] and the ability to perform phallometric testing.[188] As Daniel Scanlan observes, it is reasonable to anticipate that the general warrant "will [continue to] have broad application to the investigation of offences involving computers and the capture of data."[189]

5. Computer Searches

The addition of subsections 487(2.1) and (2.2) of the *Criminal Code* allow police to use "any computer system" to search for "any data" available to the computer system.[190] As Susan Magotiaux observes, "[t]he scope of the[se] subsection[s] ... [is] potentially boundless. ... Depending on the configurations and active connections of a given device, there could be data

---

[182] The Court found in *Tessling* that thermal imaging did not constitute a search but left open the possibility that technological advancement could lead to the opposite conclusion (see *supra* note 2 at para 55). Contrast this with the United States Supreme Court decision in *Kyllo v United States*, 533 US 27 (2001), wherein FLIR technology was found to invade a reasonable expectation of privacy. As radio frequency identification chips are now able to go "through-the-wall" (see Fontana & Keeshan, *Search and Seizure* 9th ed, *supra* note 79 at 572) and see activity inside the home, the courts will almost certainly have to revisit *Tessling*. To keep pace with developments in technology, some authors recommended that Parliament adopt FLIR warrants based on reasonable suspicion. See Steve Coughlan & Marc S Gorbet, "Nothing Plus Nothing Equals... Something? A Proposal for FLIR Warrants on Reasonable Suspicion" (2005) 23 CR (6th) 239.

[183] Although the Court in *R v Plant*, [1993] 3 SCR 281, 145 AR 104, initially determined that electrical consumption billing records did not constitute a search, the Court's more recent decision in *R v Gomboc*, 2010 SCC 55, wherein the police installed a digital recording ammeter to the powerline connected to the house, turned on the terms and conditions of the contract issued for electrical services. But for the accused not having chosen to prevent warrantless disclosure to police, a majority of the Court would have found a reasonable expectation of privacy, which would in turn have required a s. 487.01 warrant. See e.g. *R v Christensen*, 2001 ABPC 227; *R v Nguyen*, 2005 ABQB 403.

[184] See *Keating v Nova Scotia (AG)*, 2001 NSSC 85 at para 26.

[185] See Scott C Hutchison & Michael Bury, *Search and Seizure Law in Canada* (Toronto: Carswell, 1991) (loose-leaf updated 2019, release 2) ch 16 at 39. The authors cite information personally received from the Attorney General in Ontario.

[186] See *ibid*.

[187] See *Application for a General Warrant Pursuant to s 487.01 of the Criminal Code, Re*, 2002 SKPC 11.

[188] See *R v Rayworth*, [1999] OJ No 5289, 45 WCB (2d) 291 (Ont Sup Ct).

[189] Scanlan, *Digital Evidence*, *supra* note 138 at 100.

[190] "Computer system" is defined in the *Criminal Code*, *supra* note 33, s 342.1(2).

accessible to the device from other people, other networks, other countries, or other businesses."[191] The privacy interests implicated by such computer searches were aptly summarized by Justice Fish. As he wrote in *R. v. Morelli*, "[i]t is difficult to imagine a search more intrusive, extensive, or invasive of one's privacy than the search and seizure of a personal computer."[192] The need to ensure such searches respect privacy interests is therefore of the utmost importance.

Unfortunately, Parliament has not elaborated upon the process for searching computers. Indeed, until 2013 the Crown maintained that special authorizations for computer searches are unnecessary, because computers are no different than filing cabinets or cupboards.[193] Although the Court unanimously rejected these analogies,[194] by far the more difficult question requires asking *how* computer searches must be conducted.[195] This concern prompted the Court in *Vu*[196] to suggest that the broad scope of computer searches may require Parliament or the courts to devise search protocols.[197] By enacting subsections 487(2.1) and (2.2), and then refusing to update these sections in response to the Court's decision in *Vu*, Parliament has again effectively left it to the courts to determine the rules with respect to a complex search technology.

Although some commentators believe that developing computer search protocols is not possible,[198] others have proposed ways forward.[199] The capacity and functionality of modern computers give rise to some basic questions.[200] Should police be able to look through every file and folder on a computer?[201] Does the type of crime investigated limit police to reviewing

---

191 *Supra* note 14 at 510–11. The courts have confirmed the breadth of this section includes data held on computers in other physical locations. See *R v Edwards*, [1999] OJ No 3819, 44 WCB (2d) 45 (Ont Sup Ct).

192 *Supra* note 81 at para 2.

193 See *R v Vu*, 2013 SCC 60 (Factum of the Respondent at para 102) [*Vu*].

194 See *ibid* at para 24.

195 See Gerald Chan, "Life After *Vu*: Manner of Computer Searches and Search Protocols" (2014) 67 SCLR 433 at 435 [Chan, "Life After *Vu*"].

196 *Supra* note 193.

197 See *ibid* at paras 56, 62.

198 See Magotiaux, *supra* note 14 at 508; Orin S Kerr, "Ex Ante Regulation of Computer Search and Seizure" (2010) 96:6 Va L Rev 1241 at 1282 (issuing judges "cannot get a sense of the exigencies that will unfold at each stage of the search process").

199 See Chan, "Life After *Vu*", *supra* note 195 at 436.

200 See *ibid* at 436 (where the author asks these four questions).

201 The Crown has argued that officers need to cursorily inspect every file, as file names may be camouflaged. See e.g. *R v Sonne*, 2012 ONSC 1463 at paras 57–59 [*Sonne*]; *R v Bishop*, 2007 ONCJ 441 at para 47 [*Bishop*]; *R v Little*, [2009] OJ No 3278 at para 93, 87 WCB (2d) 251 (Ont Sup Ct) [*Little*].

certain types of files? Should police searches be restricted to use of certain keywords? How does the plain view doctrine operate within computer searches?[202]

It is important to explore the answers to these and related questions because leaving computer searches to ex post review is inconsistent with the purpose of section 8 of the *Charter*: to *prevent* unreasonable searches and seizures.[203] This is especially important as the case law is replete with instances where police have grossly overstepped the boundaries of what would qualify as a "reasonable" search.[204] Moreover, new technological developments allow police to search in manners much more respectful of privacy interests.[205] It is unlikely that the adversarial system will be able to stay on top of these developments, since a court's ability to respond to technological developments is limited by the evidence provided to it in a given case.[206] Parliament's approach so far has not, however, fared any better.

---

[202] For an interesting discussion of the applicability of the plain view doctrine in the context of computer searches see *R v Jones*, 2011 ONCA 632 at paras 59–70 [*Jones* ONCA]. If, for instance, the Crown is successful in arguing that police can "cursorily inspect" every file (*Sonne*, *supra* note 201; *Bishop*, *supra* note 201; *Little*, *supra* note 201), then the plain view doctrine would have nearly unlimited application.

[203] See *Hunter*, *supra* note 49 at 160.

[204] See e.g. *R v Beitel*, 2011 ONSC 5394 at paras 27–28, wherein the officer, who was looking to see if the computer was stolen, began by searching in the recycle bin, and later searched for videos. It was clear that he was looking for child pornography or other nefarious videos. Similarly, see *R v Perkins*, 2013 ONSC 1807 and *R v Boudreau-Fontaine*, 2010 QCCA 1108. Conducting computer network searches also makes the potential for over-seizure much greater. The Canadian case of *United States of America v Equinix Inc*, 2013 ONSC 193, provides a good example. In assisting the US with its investigation, Equinix was asked to send thirty-two servers worth of information to the US. The court refused to do so, as this was about one hundred full laptops worth of information. It left the parties to "agree" on narrowing the content, but if the parties failed to agree, the court would have had to deal with the order without guidance.

[205] Consider EnCase, a software device that can tell its user if any files on a computer have been altered. This may address Crown arguments that it is necessary to search all documents as criminals may "camouflage" evidence. See *Sonne*, *supra* note 201 at para 66; *Ontario (Minister of the Attorney General) v Law Society of Upper Canada*, 2010 ONSC 2150 at para 19. Similarly, a search tool known as a "file header" can tell police whether, for instance, a video image document has been disguised as a word processing document. See Christina M Schuck, "A Search for the Caselaw to Support the Computer Search 'Guidance' in *United States v Comprehensive Drug Testing*" (2012) 16:2 Lewis & Clark L Rev 741 at 750. It is also notable that in the context of the most common types of computer search investigations, child pornography, police tend to keep a large database of such videos and their "hash values" (thirty-two-digit numbers). Police can simply search for similar videos by searching hash values first, thereby preventing the need to conduct invasive searches. In a case such as *Little*, imposing a search protocol of this sort would have prevented the need to cursorily search over 13,000 files (see *supra* note 201 at para 102).

[206] See Scanlan, "Issues", *supra* note 6 at 312.

6. The Definition of "Intercept"

Although the Court reconciled the competing interpretations with respect to the meaning of "intercept" in *Jones*,[207] two main issues persist. The first concerns the prospective acquisition of "untransmitted" communications. As Professor Steven Penney observed, the definition of "private communication" should be amended "to include the prospective interception of electronic communications *before* they are transmitted."[208] Given that the current definition of "private communication" includes only "oral" communications and "telecommunications" (the latter of which requires the "emission, transmission or reception" of communicative content "by any wire, cable, radio, optical or other electromagnetic system, or by any similar technical system"), Part VI intercepts are not required to prospectively intercept non-oral communications.[209] As such, covertly installed key logger software could be used to record emails and other communications before they are sent, but these would not be afforded the protections in Part VI despite implicating identical privacy interests.[210]

Second, the result of relying on the prospective–retrospective distinction may cause constitutional issues in other contexts. In *Jones*,[211] the police had applied for a production order under section 487.012 (now 487.014) to produce historical text messages stored on Telus's database. In his concurring opinion in *Jones*, Justice Rowe raised a problem with the scheme as interpreted in Justice Cromwell's decisions in *Telus* and in *Jones*. The prospective–retrospective distinction may break down in practice, as it leaves the possibility of police applying for a transmission data warrant, and then subsequently applying for production orders to retrieve the stored messages a short time after they receive notice that a call or text was

---

[207] See *Jones* ONCA, *supra* note 202 at paras 75–77. See also Penney, "Updating Canada's Communications Surveillance Laws", *supra* note 15 at 130–34. See generally Scanlan, "Issues", *supra* note 6 at 308. There were complex technological questions about when something is "received." Relying on the prospective–retrospective distinction arguably provided a reliable means to assess whether Part VI applied.

[208] Penney, "Updating Canada's Communications Surveillance Laws", *supra* note 15 at 136 [emphasis in original].

[209] See *ibid* at 137; *Criminal Code*, *supra* note 33, s 183.

[210] See Penney, "Updating Canada's Communications Surveillance Laws", *supra* note 15 at 137, citing *United States v Scarfo*, 180 F Supp (2d) 572 at 574 (NJ Dist Ct 2001). I am unaware of any Canadian cases where police attempted to use this technology. This is likely because there is no power to do so in the *Criminal Code*, *supra* note 33. If Parliament provided such a power, this technique could, for instance, be useful in capturing passwords often required to bypass encryption technologies.

[211] *Supra* note 119.

made.[212] If the moment of authorization is what matters, then there is nothing stopping police from exploiting this loophole.[213] As I have argued elsewhere, by narrowing the definition of "intercept," the constitutional problem with its definition has simply been shifted to Parliament's production order scheme.[214]

7. Subscriber Information

In *Re Subscriber Information*,[215] the Provincial Court of Alberta considered whether subscriber information to a cell phone could be retrieved by police without warrant. Because the phone in question was internet-connected, the court concluded that its subscriber information attracted a reasonable expectation of privacy, even if the subscriber information for non-internet-connected phones did not.[216] As such, the Crown sought to have the cell phone's subscriber information produced through sections 487.016 and 487.017. To qualify, the information sought must *relate to* "telecommunication functions of dialling, routing, addressing or signalling" (487.016) or "the location of a transaction, individual or thing" (487.017). The Crown argued that cell phone subscriber information meets these tests because it is accumulated and stored to facilitate billing and collection of payment.[217] However, as subscriber information does not relate to the *functioning* of telecommunications as required by these sections, it was held not to fall within the ambit of the provisions.[218] Other cases and legal commentary support this conclusion.[219] Parliament's 2014 amendments therefore created an anomalous result by permitting police to obtain transmission and location data on a lower standard (reasonable suspicion via sections 492.1

---

212 See *ibid* at paras 83–87.

213 See *ibid*.

214 See Colton Fehr, "The Constitutionality of Using Production Orders to Obtain Stored Communications Content" (2018) 23:2 Can Crim L Rev 171.

215 2015 ABPC 178 [*Re Subscriber Info*].

216 This followed on the reasoning of *Spencer*, *supra* note 4. For decisions determining that subscriber information to regular, non-internet connected phones does not attract a reasonable expectation of privacy see *R v Khan*, 2014 ONSC 5664 at para 27; *R v Telus Communications Company*, 2015 ONSC 3964 at para 37 [*Telus* ONSC]; *HMQ and Telus Communications Company*, 2015 ONSC 3072 [*Transmission Data Recorder Warrant*].

217 See *Re Subscriber Info*, *supra* note 215 at para 19.

218 See *ibid* at paras 30–32.

219 See *Telus* ONSC, *supra* note 216 at para 53; *Transmission Data Recorder Warrant*, *supra* note 216; Randy Schwartz, "Critical Update: The Online Crime Act (Bill C-13) and New Police Search Powers" (Paper delivered during Webinar presented by Osgoode Hall Law School, 11 May 2015) [unpublished]; Marcy Henschel, "Obtaining Records of Cell Phone Calls and Text Messages" (Paper delivered at the Federation of Law Societies of Canada 42nd National Criminal Law Program, Edmonton, July 2015) [unpublished].

and 492.2) than basic subscriber information to internet-connected cell phones (reasonable and probable grounds via section 487.014).[220]

8. Summary

In most of the areas where Parliament has responded to the challenges of governing digital privacy, noticeable gaps have been revealed via judicial or academic review. Again, it is difficult to provide a definitive reason for why holes in Parliament's legislative scheme frequently arise. However, it is reasonable to conclude that in some circumstances Parliament was not provided with the relevant information when passing laws. It is likely that technology is not presented to legislators with a list of all current or possible future applications and interaction effects with other technologies. Even with the advantage of time to study technologies in depth, it is difficult to anticipate their transformative potential. Moreover, there is no guarantee that legislatures thoroughly understand digital technologies.[221] This lack of understanding has resulted in lacklustre debates that fail to expose all weaknesses in the proposed legislation.[222]

In other instances, it may be that Parliament is acting in haste or without much interest in protecting privacy. Its response to early wireless phone technology is indicative of a lack of study or outright neglect of privacy interests in early cordless telephones. Parliament's difficulties passing lawful access legislation also resulted in the Conservative government, with its first majority, taking advantage of this position by significantly expediting the legislation. In yet other instances, Parliament has made a deliberate choice to allow courts to create governing frameworks for digital technologies. The general warrant provision in section 487.01, as well as the broad computer search powers found in subsections 487(2.1) and (2.2), are illustrative. These responses demonstrate that Parliament often fails to respond adequately or intelligibly to digital privacy challenges despite its theoretical advantage over courts.

---

220 See *Re Subscriber Info*, *supra* note 215 at para 55.

221 *Cf* Solove, "Fourth Amendment", *supra* note 5 at 771 (making a similar point).

222 Although in the American context, a good example derives from Mark Zuckerberg's appearance before Congress to answer questions concerning the Facebook–Cambridge Analytica data scandal. Many of the legislators appeared to read their questions from a list provided to them. Questioners often did not have follow-up questions suggesting a lack of understanding of the issues. See ABC News, "Facebook CEO Mark Zuckerberg Testimony on Data Privacy before Senate Committee" (10 April 2018), online (video): *YouTube* <youtu.be/GQN4On0K7-w>.

C. Public Choice Theory

As discussed above, public choice theory cautions that the legislative process may be skewed in favour of powerful interest groups or majoritarian interests. As such, less fortunate groups will suffer to the benefit of those that are often wealthier, less diverse, and better organized.[223] Although Canada is generally less susceptible to the negative influences of lobbying,[224] it has been argued that novel search technologies are immune from majoritarian concerns.[225] As digital technologies are used disproportionately by the wealthy, Professor Kerr suggests that these individuals will convey their privacy interests to legislatures, "resulting in a healthy debate and relatively favorable conditions for balanced legislative rules."[226] These contentions have not, however, been tested in the Canadian digital privacy and criminal procedure contexts.

The lawful access experience provides an illuminating case study for investigating the influence (or lack thereof) of lobbyists and majoritarian politics on digital privacy rules. In Parliament's first review of the issues surrounding lawful access, it consulted more than three hundred organizations ranging from police services, telecommunications service providers (TSPs), civil rights groups, and individual Canadians.[227] As a result of this

---

[223] See Penney, "Reasonable Expectations", *supra* note 14 at 503, citing Kent Roach, *Due Process and Victims' Rights: The New Law and Politics of Criminal Justice* (Toronto: University of Toronto Press, 1999); William J Stuntz, "The Pathological Politics of Criminal Law" (2001) 100:3 Mich L Rev 505 at 553–56.

[224] See Raj Chari, Gary Murphy & John Hogan, "Regulating Lobbyists: A Comparative Analysis of the United States, Canada, Germany and the European Union" (2007) 78:3 Political Q 422 at 432; Barrie McKenna, "Corrupt Canada? We're Small Time Compared to the US", *The Globe and Mail* (10 October 2010), online: <www.theglobeandmail.com> [perma.cc/B9U8-KVUW]. The evidence that private actors have successfully lobbied Parliament in the digital privacy context is thin. My review of the available literature and parliamentary debates led to only one feasible example: the motivation behind enacting section 184.5 of the *Criminal Code*. This section allows interception of radio-based communications commonly conducted via early models of cordless and cellular phones but prohibits malicious or profitable disclosure of such communications. The accusation was that telecommunications companies would prosper by having looser privacy protections in the area of radio-based cellular and cordless phone communications, which constituted millions of users at that time. Consumers who value their privacy are much more likely to buy added encryption protection than they would if that protection was provided by law. The opposition parties strongly suggested that banning scanners used to intercept communications was a much more reasonable way of protecting privacy interests. The Conservative government did not, however, see a problem with its legislation being directly aimed at helping telecommunications companies "prosper." See "Bill C-109, An Act to amend the Criminal Code, the Crown Liability and Proceedings Act and the Radiocommunication Act", *House of Commons Debates*, 34-3, vol 13 (26 February 1993) at 16558–-62, 16655.

[225] See Kerr, "Fourth Amendment", *supra* note 5 at 887.

[226] *Ibid*.

[227] See *Legislative Summary of Bill C-74*, *supra* note 122 at C(1).

consultation, Parliament tabled Bill C-74 in 2005 only to have it die on the order table due to an election being called.[228] As mentioned earlier, subsequent attempts to pass lawful access legislation were made in 2009, 2010, and 2012. These proposals did not make it past first reading. The 2014 proposals found in Bill C-13, however, were passed by a majority Conservative government.

Throughout this experience the federal government justified increased lawful access demands by appealing to the need to protect Canadians from terrorists, identify pedophiles, prosecute violent offenders, and address the issue of cyberbullying.[229] However, the various lawful access proposals were met with fierce opposition from civil rights groups, privacy commissioners, academics, and at times TSPs.[230] The TSPs questioned the need for broad access powers, and also raised the more self-interested question of who would incur the costs of installing the necessary infrastructure to provide government access.[231] Civil rights groups rapidly disseminated information to the public via the media to create an atmosphere of opposition to controversial aspects of each attempt to institute lawful access legislation.[232] Opposition parties also seized on the opportunity to critique the Conservatives for pandering to law enforcement demands.[233]

---

228 See Daphne Gilbert, Ian R Kerr & Jena McGill, "The Medium and the Message: Personal Privacy and the Forced Marriage of Police and Telecommunications Providers" (2006) 51 Crim LQ 469 at 483.

229 See Parsons, "Stuck on the Agenda", *supra* note 30 at 262, citing Canada, Department of Justice, "Summary of Submissions to the Lawful Access Consultation: Lawful Access FAQ" (2005), online: *Department of Justice* <www.justice.gc.ca> [perma.cc/2UG9-MSGS]; Jesse Kline, "Vic Toews Draws Line on Lawful Access: You're with Us, or the Child Pornographers", *National Post* (14 February 2012), online: <www.nationalpost.com> [perma.cc/Y3LG-ZGU3]; Daniel Proussalidis, "Magnotta to Be Charged with Criminal Harassment of PM", *Winnipeg Sun* (1 June 2012), online: <www.winnipegsun.com> [perma.cc/9BW4-BFFV]; Tabatha Southey, "Bill C-13 Is About a Lot More than Cyberbullying", *The Globe and Mail* (6 December 2013), online: <www.theglobeandmail.com> [perma.cc/6AM4-9AQ7].

230 See Parsons, "Stuck on the Agenda", *supra* note 30 at 262–63.

231 See *ibid* at 263, citing Canada, Parliamentary Information and Research Service: Law and Government Division, *Telecommunications and Lawful Access: I. The Legislative Situation in Canada*, by Dominique Valiquet, Catalogue No PRB 05-65E (Ottawa: Library of Parliament, 2006), online (pdf): <publications.gc.ca/collections/collection_2007/lop-bdp/prb/PRB0565-e.pdf>; Nestor Arellano, "Small ISPs Foresee Cost Burden in 'Lawful Access' Bills" (27 June 2011), online: *ITBusiness* <www.itbusiness.ca> [perma.cc/MG3L-B7SQ]; Christopher Parsons, "Unpacking the Potential Costs of Bill C-30" (2012) 9:6 Can Privacy L Rev 57.

232 See Parsons, "Stuck on the Agenda", *supra* note 30 at 263.

233 See *ibid*, citing Lindsey Pinto, "NDP Leader Responds to StopSpying.ca Campaign" (25 May 2012), online: *OpenMedia* <openmedia.org> [perma.cc/WF9B-QV3E].

The impact of civil society's opposition could be seen throughout the process. As Parliament admitted in its legislative backgrounder to Bill C-74, the creation of storage obligations requiring TSPs to collect and store information about their customers' internet viewing histories was not included after its initial consultation.[234] This is contrary to numerous regimes in Europe, which have such data retention policies.[235] A national database storing names and addresses of customers was also not part of Bill C-74.[236] Nor was a "know your customer" requirement. This would require knowing the identity of who was purchasing a service, which would prevent retailers from selling items such as anonymous phone cards.[237] The concerns raised by privacy advocates dissuaded Parliament from acceding to law enforcement requests to implement these anti-privacy policies.[238]

With these initial concessions, Parliament slimmed down its first proposal in Bill C-74. It maintained, however, a requirement that TSPs update their infrastructure to allow police to intercept communications.[239] It also included a provision allowing law enforcement to obtain ISP subscriber information upon request, without judicial authorization.[240] This law was designed to provide the "lawful authority" required under paragraph 7(3)(c.1) of *PIPEDA* to allow TSPs to hand over subscriber information without warrant.[241] As some authors observed at the time, this development would lead to "a significant alteration in the procedural safeguards against excessive fishing expeditions by law enforcement agencies."[242] The fact that the legislation provided no overview for this process made this proposal even more controversial.[243] As a result, privacy advocates protested the bill, only to have it die on the order table following the calling of an election.

---

234 See *Legislative Summary of Bill C-74*, *supra* note 122 at D(1).

235 See Ann Cavoukian, "Privacy, Transparency, and the Rule of Law: Critical to Preserving Freedom and Liberty" (2005) 19 NJCL 193 at 210, citing Robert Wielaard, "Data Retention Bill Divides EU Countries", *SFGate.com* (8 September 2005); "U.K. Sets Out Case for Data Logs to Fight Terror", *Yahoo News* (*Reuters*) (7 September 2005); "EU Data Protection Chief Warns Against Anti-Terrorism Plans", *Mercury News* (26 September 2005); *Legislative Summary of Bill C-13*, *supra* note 143 at 2.1.11.

236 Law enforcement specifically wanted this addition. See *Legislative Summary of Bill C-74*, *supra* note 122 at subheading "(A)" under the heading "Commentary."

237 See *ibid* at D(2).

238 See *ibid*. See also Michael Geist, "Ottawa Finds Public No Pushover in Snooping Law", *Toronto Star* (30 October 2006) at E3.

239 See Bill C-74, *supra* note 101, cl 7.

240 See *ibid*, cl 17.

241 See *supra* note 130. See generally *Spencer, supra* note 4.

242 Gilbert, Kerr & McGill, *supra* note 228 at 486.

243 See Parsons, "Stuck on the Agenda", *supra* note 30 at 264, citing Philippa Lawson, *Moving Towards a Surveillance Society: Proposals to Expand "Lawful Access" in Canada* (Vancouver: British Columbia Civil Liberties Association, 2012) at 6.

The 2009, 2010, and 2012 attempts to pass lawful access legislation suffered from the same controversial aspects of Bill C-74.[244] The battle was again fought in the media, wherein civil rights groups and opposition parties aligned themselves against the government proposal. A series of social media campaigns was highly influential at painting the government's bill as anti-privacy.[245] The opposition parties also launched campaigns against each bill.[246] In so doing, they accused the Conservatives of pandering to majoritarian desires to be "tough on crime" as opposed to drafting a constitutionally compliant lawful access scheme that took seriously the many concerns raised by pro-privacy advocates.[247]

Even TSPs played an active role in opposing the new legislation. The federal government had proposed modifications to the *Solicitor General's Enforcement Standards (SGES) for Lawful Interception of Telecommunications* that would require licensed TSPs to replace circuit switched telephony systems with interconnected radio-based transmission facilities.[248] As the TSPs' representative observed, this change "opens up several additional services to interception requirements, including Internet services, and cable and broadcasting services."[249] The TSPs objected since this strategy sought to do with regulations what Parliament had been unable to accomplish with its legislation.[250] Even without significant response from the other privacy advocates, the federal government backed off from this proposed change.

---

244 *Supra* notes 102–05.

245 See Jesse Brown, "Slacktivism Defeats Lawful Access", *Maclean's* (21 September 2011), online: <www.macleans.ca> [perma.cc/4K3F-583G]; Laura Stone, "Conservatives Kill Internet Surveillance Bill C-30", *iPOLITICS* (11 February 2013), online: <www.ipolitics.ca> [perma.cc/6J3K-J3DB]; Laura Payton, "Internet Privacy Experts Raise Concerns over Crime Bill", *CBC News* (9 August 2011), online: <www.cbc.ca> [perma.cc/R79U-DYDG]; "A Look Back at Our Campaign Against Canada's Bill C-30" (last visited 5 March 2019), online: *OpenMedia* <openmedia.org> [perma.cc/YC27-AQVR]; Laura Payton, "'Tell Vic Everything' Tweets Protest Online Surveillance" *CBC News* (16 February 2012), online: <www.cbc.ca> [perma.cc/KE76-E2B4].

246 See Parsons, "Stuck on the Agenda", *supra* note 30 at 267, citing Liberal Party of Canada, "Don't Let Harper Read Your Emails" (2013), online: <petition.liberal.ca> [perma.cc/3CFB-ENPA] and a personal interview with Steve Anderson in 2013.

247 See e.g. Bill C-46, Debate, *supra* note 162 at 6186; Bill C-47, Debate, *supra* note 164 at 6251.

248 See Canadian Wireless Telecommunications Association, "Re: Consultation on a Licensing Framework for Mobile Broadband Services (MBS) — 700 MHz Band", *Canadian Radio-television Telecommunications Commissioner* (22 June 2012), online (pdf): <www.ic.gc.ca> [perma.cc/4LB4-WMTC].

249 *Ibid* at 4.

250 See *ibid*.

The result of the decade-long debate on lawful access was that the government conceded that any modernization to police powers would not include "the warrantless mandatory disclosure of basic subscriber information or the requirement for telecommunications service providers to build intercept capability within their systems."[251] However, one controversial aspect remained in the legislation Parliament passed—namely, section 487.0195—which allows TSPs to voluntarily disclose subscriber information to law enforcement without incurring civil or criminal liability. However, as the Court in *Spencer* recognized a reasonable expectation of privacy in ISP subscriber information, it is unlikely that telecommunications providers will risk their reputations and provide such information to police without a warrant.[252] The lawful access experience thus exemplifies the ability of civil society to mobilize to protect digital privacy interests, even in the face of persistent demands by law enforcement for expansive search powers and a government using majoritarian "tough on crime" politics to achieve political ends.

III. Implications

The above review suggests that Parliament's advantage over courts in responding to complex and rapidly changing search technologies is more theoretical than real. Although Parliament should be able to respond quickly and coherently, it often fails to meet these objectives. It is notable, however, that there appear to have been few instances where public choice concerns have given rise to serious problems in the context of criminal law legislation governing digital technologies. Any proposal, then, needs to begin by recognizing that in the criminal law and digital privacy contexts, both courts and Parliament are slow in responding; both also make rules in incomplete information environments, but tend to make them in an even-handed manner.

Two other points must also affect any institutional strategy. First, Parliament has exclusive authority to pass new offences or update current offences. As such, it is Parliament's sole prerogative to carefully tailor the definition of offences to keep up with digital technologies—a task that has proven to be quite challenging. Second, courts often serve a gap-filling role when developing and implementing rules governing complex and rapidly changing search technologies. The challenge is therefore twofold. First, how should Parliament tailor its non-offence related legislation knowing that it tends to react slowly and at times incoherently? Second, how can we best ensure that courts play their gap-filling role most effectively?

---

[251] Laura Payton, "Government Killing Online Surveillance Bill", *CBC News* (11 February 2013), online: <www.cbc.ca> [perma.cc/L2EZ-KGFC].

[252] See *Re Subscriber Info*, *supra* note 215 at para 14.

Any approach to governing digital privacy should begin by considering the literature on institutional choice. Professors Neil Komesar and Adrian Vermeule have each written on this topic.[253] They recognize that "comparing institutions requires identifying parallels across institutions in some acceptable, understandable, and usable fashion."[254] To accomplish this end, Professor Komesar developed the "participation-centred approach."[255] The model is a simple economic one wherein "[t]he character of institutional participation is determined by the interaction between the benefits of that participation and [its costs]."[256]

One of the major impediments for using courts was discussed above—namely, judicial ability to receive adequate information. Another barrier is litigation costs, how they are diffused, and whether they create incentives to litigate.[257] Professor Komesar uses pollution as his primary example to illustrate when these considerations might influence institutional approaches to rulemaking. If everyone faces small losses for pollution, no individual lawsuits will arise, and unless the amount of damages is large overall, there likely will not be a class action.[258] Moreover, preventing pollution is extremely complex. A similar logic could be applied to the digital privacy context. Given the ability of legislatures to thoroughly research an issue, legislatures are better suited to weigh the competing concerns. As long as there are not significant majoritarian or lobbying concerns, it is best to leave it to the legislature.

As Professor Vermeule observes, however, institutional choice is also determined by a country's constitutional and institutional arrangements and cultures.[259] In addition to the fact that Professor Komesar is speaking in the American setting, the examples he used are not applicable in the narrower topic of this article for two reasons. First, the potential for exclusion of evidence in the criminal law context always provides an incentive to litigate vague or yet-to-be-determined police powers, even if the violation seems small.[260] Second, although public choice concerns have proven to be insignificant, Parliament has been at least as slow and confusing in passing legislation as courts have been in developing the common law. Although it

---

253 See Komesar, *supra* note 28; Adrian Vermeule, *Judging Under Uncertainty: An Institutional Theory of Legal Interpretation* (Cambridge, Mass: Harvard University Press, 2006).

254 Komesar, *supra* note 28 at 7. See generally Vermeule, *supra* note 253 at 74–75.

255 Komesar, *supra* note 28 at 7.

256 *Ibid* at 8.

257 See *ibid* at 25.

258 See *ibid*.

259 See Vermeule, *supra* note 253 at 75, 284.

260 As is possible under section 24(2) of the *Charter, supra* note 17.

is often assumed that legislatures will utilize their institutional advantages, the Canadian digital privacy and criminal law contexts provide an excellent example of Parliament being unable to take advantage of its institutional strengths.

It is therefore appropriate to be skeptical about the utility of relying on institutional competence arguments as the sole means for determining the appropriate role of each institution when governing digital privacy. As one critic of institutional choice theory observes, relying on broad generalizations of institutional competence paints "a stilted portrait of institutions" that "focuses too heavily on the current characteristics of institutions rather than on their potential for reform and change."[261] In other words, the "inherent" strengths and weaknesses of courts and legislatures are subject to ebb and flow. This in turn affects each institution's ability to respond effectively at different times. A better approach, then, would focus on how these institutions can work together to respond to the various challenges.[262] I suggest this approach can be applied to governing digital privacy.

To begin furthering this aim, I have elsewhere developed two institutional strategies to aid Canadian courts in developing digital privacy rules.[263] The first proposal concerns scenarios where Parliament—either intentionally or inadvertently—leaves it to the courts to develop a rule to govern a complex and rapidly advancing technology. In broad strokes, I suggest that when Parliament relies on courts to play such a role, it should send the relevant question as a reference to the Supreme Court or other provincial appellate courts.[264] The reference process not only allows appellate courts to develop rules with an ideal evidentiary record,[265] but also avoids lengthy trial and appeal delays.[266] In other words, utilizing the reference procedure allows courts to provide an informed and timely response to a digital privacy issue.

---

[261] Daniel J Solove, "The Darkest Domain: Deference, Judicial Review, and the Bill of Rights" (1999) 84:5 Iowa L Rev 941 at 1011.

[262] *Cf* Murphy, *supra* note 5 at 534. Murphy's proposal looks very different from mine—what she calls "collaboration" effectively requires courts to show extreme deference (see *ibid* at 537–44).

[263] See Colton Fehr, "Digital Evidence and the Adversarial System: A Recipe for Disaster?" (2018) 16:2 CJLT 443 [Fehr, "Digital Evidence"].

[264] See *ibid*. I use judicial development of the law concerning cell phone searches incident to arrest to illustrate how the many misunderstandings of cellular technologies impacted how courts decided whether/how such a search ought to be permitted. Had the issue been sent to the Court as a reference, I contend that the reference procedure would have allowed the Court to correct the technological assumptions underlying earlier decisions.

[265] See *ibid*. For instance, the *Supreme Court Act*, RSC 1985, c S-26, ss 53–55, 87, allows the Court to call any witnesses or rely on any documents it deems necessary to develop the evidentiary record.

[266] See Fehr, "Digital Evidence", *supra* note 263.

To help courts apply existing rules to digital technologies, I recommended tasking an independent institution with an investigative role.[267] By providing reports outlining timely and pertinent facts related to technologies expected to come before the courts, counsel would have reliable information upon which to argue its case.[268] In turn, digital privacy rules would be much more likely to be applied in a principled manner.[269] Even if the ultimate ruling is of little precedential value due to technology outpacing the law, the decision will at least have been made with a robust evidentiary record and thus stand a much greater chance of being consistent with *Charter* principles.[270]

These reforms, however, do not address how Parliament should tailor its digital privacy legislation. As section 8 of the *Charter* requires that searches be authorized by law, Parliament must typically pass a law granting search powers to law enforcement.[271] Although Parliament may provide courts with broad legislation like the general warrant provision (section 487.01) or computer search provisions (subsections 487(2.1) and (2.2)), ex post judicial development of such rules is not an optimal procedure because it fails to communicate the rule before a technology is in widespread use. Legislative rules are thus preferable to the extent that they can provide clear and lasting guidance to law enforcement officers before searches of a technology become common.

In deciding how a law affecting digital privacy should be drafted, Parliament should therefore consider the relative costs of specific and general rules. As discussed earlier, when Parliament passes detailed legislation with respect to complex and rapidly advancing technologies, those laws tend to become outdated or have gaps which either needlessly undermine privacy or unduly hamper police investigations. Where the technology is stable, however, legislative rulemaking can better respond to both law enforcement and privacy interests. This follows because stable technologies can be studied in depth and rules can be crafted without concern that the law will soon become outdated. Delays inherent in the adversarial process

---

267 See *ibid*. I suggest that a suitable candidate would be the Office of the Privacy Commissioner.

268 See *ibid*. For an example of what such a report would look like, see Office of the Privacy Commissioner of Canada: Technology Analysis Branch, *What an IP Address Can Reveal About You* (Ottawa: Office of the Privacy Commissioner of Canada, 2013), online: <www.priv.gc.ca> [perma.cc/2Z3U-ZE43].

269 See Fehr, "Digital Evidence", *supra* note 263.

270 See *ibid*.

271 See *Collins*, *supra* note 64 at 278. Common law searches (such as investigative detentions and searches incident to arrest) are exceptions.

will result in judicial rules relating to stable technologies being unknown for unnecessarily lengthy periods of time.[272]

Where Parliament is unsure about the development of a technology, however, legislative rules are vulnerable to becoming quickly outdated. To address this concern, Parliament should approach drafting its legislation in one of two ways. First, it could draft digital privacy laws broadly and allow courts to update the law on a case-by-case basis. If my above recommendations allow courts to receive adequate information about digital technologies, courts will be well equipped to develop principled digital privacy rules. Although this approach would likely result in many rules lagging behind technological development, this is already a prominent feature of legislative and judicial digital privacy rules in the digital privacy and criminal law settings.

Second, if Parliament is confident in its understanding of a complex and rapidly advancing technology and its ability to pass a rule expediently, it could consider passing rules with built-in sunset clauses.[273] By ensuring that a rule is no longer applicable after a designated period, Parliament can control, to some extent at least, whether its legislation will be overtaken by technological advancement. Moreover, sunset clauses can be designed to ensure that the law comes before a special committee tasked with reporting to Parliament before the law expires.[274] Parliament can then take the opportunity to consider any potential gaps in its legislation and respond accordingly.

This more dynamic approach to governing digital privacy requires that courts and legislatures be flexible in determining the process for making a rule. There are multiple options for crafting principled rules and some processes may prove more or less feasible at different times due to restrictions in the judicial and political processes. The ideal approach would allow Parliament to craft and expediently revisit digital privacy rules in a way that allows for judicial review of its legislation. Recognizing that this is unlikely to occur frequently, Parliament must be attuned to its institutional weaknesses, and focus on strengthening the judicial process to allow the courts to address the inevitable gaps that its legislation will leave. The above recommendations, I suggest, would go a long way in achieving these goals.

Several objections to this proposal may be anticipated. First, it may be argued that stare decisis will prevent courts from responding flexibly to

---

[272] Although such issues could be sent to the Court via reference, it is implicit in my reference suggestion that this process be used only where regular legislative and judicial processes are likely to fail.

[273] See e.g. Kerr, "Fourth Amendment", *supra* note 5 at 871.

[274] See e.g. Canada, Department of Justice, "About the Anti-Terrorism Act" (26 July 2017), online: *Department of Justice* <www.justice.gc.ca> [perma.cc/6K46-C2DR].

technological change.[275] It should be remembered, however, that developing digital privacy rules in the criminal procedure context implicates section 8 of the *Charter*. As the Court recently concluded, significant factual changes underlying *Charter* decisions make it permissible for lower courts to reconsider even the Supreme Court's rulings.[276] Although the Court has cautioned against liberal use of this exception,[277] it is not difficult to imagine changes in technology "fundamentally shifting" the applicable privacy and security interests central to determining whether a search or seizure is unreasonable. As such, stare decisis should not prove as restrictive as it may be in other contexts or countries.[278]

Second, any suggestion that Parliament should play a lesser role in developing police search powers is constitutionally questionable. As Professor James Stribopoulos observes, the principle of legality requires that police powers derive from Parliament, not from the courts.[279] The legality principle does not, however, inhibit Parliament from passing broad legislation to facilitate judicial development of digital privacy rules. First, it is notable that the Court has, for better or for worse, all but abandoned the legality principle by creating a variety of police powers under the common law.[280] Second, although searches must, at minimum, be authorized by law,[281] the courts have not imposed a high threshold for meeting this requirement. For instance, the broadest provision discussed above—the general warrant found in section 487.01—has survived constitutional scrutiny on this ground.[282] As such, there does not appear to be a constitutional impediment to my proposal.

Finally, it may be argued that it is undemocratic to vest significant digital privacy rule-making duties with courts. This argument may be countered in two ways. First, it is notable that those advocating for legislative primacy in the fields of digital privacy and criminal law do not present any cogent arguments to address the significant limitations of legislative rule-

---

[275] See e.g. Kerr, "Fourth Amendment", *supra* note 5 at 871.

[276] See *Canada (AG) v Bedford*, 2013 SCC 72 at para 44.

[277] See *R v Comeau*, 2018 SCC 15 at paras 30–34.

[278] See Kerr, "Fourth Amendment", *supra* note 5 at 871, where the author discusses the American context.

[279] See James Stribopoulos, "In Search of Dialogue: The Supreme Court, Police Powers, and the *Charter*" (2005) 31:1 Queen's LJ 1.

[280] See *ibid* at 2–3. See also Tim Quigley, "*R v Fearon*: A Problematic Decision" (2015) 15 CR (7th) 281, citing Tim Quigley, *Procedure in Canadian Criminal Law* (Toronto: Carswell, 2005) (loose-leaf) at 5-34 to 5-46.

[281] See *Collins*, *supra* note 64 at 278.

[282] See *Lucas*, *supra* note 181 at paras 104–26; *Kuitenen*, *supra* note 181 at para 4. For academic criticism see Coughlan, *Criminal Procedure*, *supra* note 181 at 133–34.

making.[283] Political science scholars observe that politicians tend to address issues only when they arise on the public agenda.[284] Whether a legal gap will be addressed in turn depends on what other issues of the day are demanding political attention.[285] Moreover, the fact that Canadian federal governments are often in minority positions makes passing legislation with any controversy increasingly difficult.[286] Add to this the necessary study required to pass legislation, as well as laws having to pass through both the House of Commons and the Senate. There are also temporal and practical barriers that often become insurmountable for both minority and majority legislatures.[287] Parliament should acknowledge these limitations and explore institutional options to address them. This does not strike me as undemocratic: it exemplifies responsible governance.

Second, my proposal need not stifle Parliament from passing digital privacy laws or prevent Parliament from responding to digital privacy rulings. Instead, I suggest that Parliament should consider its institutional limitations before passing digital privacy legislation. This still allows for important dialogue on the content of rights to occur.[288] As Professor Peter Hogg and Allison Bushell observe, the democratic legitimacy of judicial review is bolstered because the structure of the *Charter* often results in judicial review of legislation leaving room for a legislative response.[289] That response is typically able to achieve the legislature's objective while at the same time respecting constitutional rights.[290] In this way, then, constitu-

---

283 See especially Kerr, "Fourth Amendment", *supra* note 5.

284 See Parsons, "Stuck on the Agenda", *supra* note 30 at 258–61 for a literature review on agenda setting.

285 See *ibid*. As the author notes, the public agenda tends to attract no more than five to seven issues at a time.

286 The lawful access experience is exemplary.

287 See Solove, "Fourth Amendment", *supra* note 5 at 771 (making a similar argument in the American context).

288 See generally Peter W Hogg & Allison A Bushell, "The *Charter* Dialogue Between Courts and Legislatures (Or Perhaps the *Charter of Rights* Isn't Such a Bad Thing After All)" (1997) 35:1 Osgoode Hall LJ 75. See Peter W Hogg, Allison A Bushell Thornton & Wade K Wright, "*Charter* Dialogue Revisited—Or 'Much Ado About Metaphors'" (2007) 45:1 Osgoode Hall LJ 1.

289 See Hogg & Bushell, *supra* note 288 at 79–80. See also Kent Roach, *The Supreme Court on Trial: Judicial Activism or Democratic Dialogue* (Toronto: Irwin Law, 2001) at 11 [Roach, *The Supreme Court on Trial*].

290 See Roach, *The Supreme Court on Trial*, *supra* note 289 at 12. As Professor Kent Roach observes, the ability of *Charter* dialogue to place issues on the legislative agenda improves democracy by ensuring that controversial issues are subject to robust public debate (see Kent Roach, "Dialogic Judicial Review and Its Critics" (2004) 23 SCLR (2d) 49 at 75 [Roach, "Dialogic Judicial Review").

tional dialogue provides an important mechanism for determining "how society should struggle together for the best answers to controversies about justice."[291]

As should be evident from Part II, dialogue in the digital privacy context has been lacklustre.[292] This should not be surprising. Courts and legislatures are having difficulty determining the basic facts upon which to create rules governing digital technologies. They are also having difficulty keeping pace with the rapid development of digital technologies. Dialogue is meaningless if there is no basic understanding of what facts underlie the dialogue or if the dialogue is rendered moot because a rule becomes outdated due to its failure to keep pace with use of a particular technology. By reforming how courts receive information about digital technologies, courts will become equipped to participate in this dialogue.

Parliament's "tone" in this dialogue should, however, be altered to reflect the changing circumstances within which this conversation takes place. A revitalized dialogue in the digital privacy context requires that Parliament pay attention to judicial and legislative weaknesses in rule-making. In practice, this will often require Parliament to speak more cautiously, using tools such as sunset clauses to ensure its legislation does not unduly hinder law enforcement or needlessly undermine digital privacy. This modified approach to passing digital privacy laws, I suggest, provides a democratically responsible way of ensuring that Canadian institutions tasked with governing digital privacy are capable of balancing the important law enforcement and digital privacy interests at the heart of section 8 of the *Charter*.

Conclusion

American scholars have entertained a lively debate about the relative institutional capacities of legislatures and courts to govern privacy interests in light of rapidly evolving and complex search technologies. Although the Canadian judiciary has encountered similar problems as their American counterparts, a comprehensive study had not been undertaken to assess the potential advantages of having Canadian legislatures govern digital technologies. This article fills the void with respect to the institutional capacities of Parliament to govern digital privacy in the criminal law context. After reviewing several decades of its legislation, I conclude that there is little reason to believe that Parliament is quicker or more coherent in its

---

[291] Roach, "Dialogic Judicial Review", *supra* note 290 at 104.

[292] For example, Parliament has not responded to the Court's decisions concerning ISP subscriber information, the definition of intercept, computer searches, and searches of cell phones incident to arrest.

responses to digital technologies than courts. Unlike with Congress, however, concerns about Parliament being susceptible to majoritarian or lobbyist influence are minor. This may be the result of the more stable political climate in Canada, or, as Professor Kerr contends, because the populace is more likely to defend its digital privacy interests given their general importance to the polity.[293]

The research findings in this article directly inform my proposed institutional approach for governing digital privacy in the Canadian criminal law context. As courts and Parliament have similar weaknesses, it is not sensible to rely on institutional process arguments to exclude one institution from governing digital privacy. Instead, the focus should be on how to help courts and legislatures work together to ensure the best digital privacy rules are implemented. This requires thinking creatively about how to address institutional weaknesses. In addition to ensuring courts are institutionally equipped to respond to digital privacy concerns, Parliament should be vigilant about weighing the costs and benefits of responding to novel and complex technologies with legislation. When a technology is advancing quickly, Parliament can either pass broad laws that allow judges to fill in legislative gaps or proceed cautiously, using tools such as sunset clauses to ensure its legislation is not vulnerable to falling out of date. Although this approach may abdicate significant rule-making authority to courts, concerns about democratic legitimacy are mitigated if Parliament approaches digital privacy rule-making with a realistic assessment of its capacity to meet the challenges of governing privacy in the digital age.

---

[293] See Kerr, "Fourth Amendment", *supra* note 5.