The Supreme Court Law Review: Osgoode's Annual Constitutional Cases Conference

Volume 67 (2014) Article 16

The Digitization of Section 8 of the Charter: Reform or Revolution?

Steven Penney

Citation Information

Penney, Steven. "The Digitization of Section 8 of the Charter: Reform or Revolution?." *The Supreme Court Law Review: Osgoode's Annual Constitutional Cases Conference* 67. (2014).
http://digitalcommons.osgoode.yorku.ca/sclr/vol67/iss1/16

The Digitization of Section 8 of the Charter: Reform or Revolution?

Steven Penney[*]

I. INTRODUCTION

Police have conducted searches and seizures of computers and other digital devices[1] for some time.[2] But the ubiquity, portability, connectivity, and processing and storage capacities of contemporary devices[3] present new challenges to the law of search and seizure, including the interpretation and application of section 8 of the *Canadian Charter of Rights and Freedoms*, which guarantees everyone's "right to be secure against unreasonable search or seizure".[4]

For some, digitization is a grave threat to the socio-legal order. Law enforcement officials complain that criminals' use of technology has outstripped the investigative capacity of police and plea for legislators and judges to restore the pre-digital status quo.[5] Privacy advocates also

---

[*] Faculty of Law, University of Alberta.

[1] The terms "computer" and "digital device" are used interchangeably in this paper. In the *Criminal Code*, a "computer system" is defined for various purposes as "a device that, or a group of interconnected or related devices one or more of which, (a) contains computer programs or other data, and (b) pursuant to computer programs, (i) performs logic and control, and (ii) may perform any other function". This definition would seem to encompass virtually any digital device, including desktop, laptop, and tablet computers, mobile phones, and related technologies. *Criminal Code*, R.S.C. 1985, c. C-46, s. 342.1(2).

[2] See, *e.g.*, *R. v. DeCoste*, [1983] N.S.J. No. 516, 60 N.S.R. (2d) 170 (N.S.S.C. (T.D.)) (search warrant for computerized hospital records); *R. v. Cardoza*, [1981] O.J. No. 3258, 61 C.C.C. (2d) 412 (Ont. Co. Ct.) (search of computerized telephone records).

[3] See generally Viktor Mayer-Schonberger & Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Boston: Houghton Mifflin Harcourt, 2013), at 9 (noting that stored information grows four times faster than the world economy, and computer processing power nine times faster).

[4] Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11 [hereinafter "Charter"].

[5] See, *e.g.*, Canadian Association of Chiefs of Police, "Police Confirm Canadians' Top Five Fears about Lawful Access" (October 26, 2012), online: <http://www.cacp.ca/media/news/download/1363/Final_CACP_Press_Release_-_Lawful_Access.pdf>; Department of Justice Canada,

yearn for restoration, but they claim digitization has been a boon for state surveillance and demand legislation and court rulings forestalling Big Brother's advance.[6]

The aim of this paper is not to resolve this debate. Indeed, given people's divergent interests[7] and dispositions,[8] "privacy versus security" is likely to be a perpetually polarizing dialectic. But a narrower question might be resolved: does digitization require a fundamental conceptual overhaul of section 8 doctrine, or is that doctrine reasonably well equipped to accommodate the digital revolution?

I favour the latter response. There is little reason to think that digitization requires a radical reinterpretation of section 8.[9] Technological change inevitably influences constitutional interpretation and application.[10] But for the most part, the foundation set out by the Supreme Court of Canada in digital (and other) section 8 cases over the past two decades provides the conceptual and doctrinal tools needed to achieve reasonable

---

"Summary of Submissions to the Lawful Access Consultation" (April 28, 2003), at 11-19, online: <http://www.justice.gc.ca/eng/cons/la-al/sum-res/sum-res.pdf>; Susan Landau, *Surveillance or Security?: The Risks Posed by New Wiretapping Technologies* (Cambridge, MA: MIT Press, 2010), at 7.

[6] See, *e.g.*, Kevin Haggerty, "Methodology as a Knife Fight: The Process, Politics and Paradox of Evaluating Surveillance" (2009) 17 Crit. Criminol. 277; Jena McGill & Ian Kerr, "Reduction to Absurdity: Reasonable Expectations of Privacy and the Need for Digital Enlightenment" (2012) Digital Enlightenment Yearbook 199.

[7] See generally Meredith Kapushion, "Hungry, Hungry HIPPA: When Privacy Regulations Go Too Far" (2003) 31 Fordham Urb. L.J. 1483, at 1491: "Consumers have wildly divergent preferences based on their individual needs and tempered by the costs they are willing to bear."

[8] See generally Darhl M. Pedersen & Shelia Frances, "Regional Differences in Privacy Preferences" (1990) 66 Psych Reports 731 (reviewing psychological literature finding marked differences in privacy preferences depending on numerous personal characteristics and situational factors); Ponnurangam Kumaraguru & Lorrie Faith Cranor, "Privacy Indexes: A Survey of Westin's Studies" (2005) Carnegie Mellon University, Institute for Software Research International, online: <http://reports-archive.adm.cs.cmu.edu/anon/isri2005/CMU-ISRI-05-138.pdf> (finding shifting proportions of U.S. population characterized as "privacy fundamentalists" (approximately one-quarter to one-third), "privacy pragmatists" (over one-half), and "privacy unconcerned" (around one-tenth)). As mentioned *infra* note 127, however, empirical researchers have found that people's survey-expressed privacy preferences are often belied by their observed behaviours.

[9] For commentary taking a more radical approach, see, *e.g.*, Matthew Johnson, "Privacy in the Balance: Novel Search Technologies, Reasonable Expectations, and Recalibrating Section 8" (2012) Crim. L.Q. 442; Jane Bailey, "Framed by Section 8: Constitutional Protection of Privacy in Canada" (2008) Can. J. Crim. & Crim. Jus. 279; Lisa M. Austin, "Information Sharing and the 'Reasonable' Ambiguities of Section 8 of the Charter" (2007) 57 U.T.L.J. 499.

[10] See generally Lawrence H. Tribe, "The Constitution in Cyberspace: Law and Liberty Beyond the Electronic Frontier" in David M. Kaplan, ed., *Readings in the Philosophy of Technology*, 2d ed. (Lanham: Rowman & Littlefield, 2009) 309; Thomas Fetzer & Christopher S. Yoo, "New Technologies and Constitutional Law" in Mark Tushnet, Thomas Fleiner & Cheryl Saunders, eds., *Routledge Handbook of Constitutional Law* (New York: Routledge, 2013) 485.

accommodations between competing privacy and law enforcement interests in the digital era.

The remainder of the paper consists of five parts. I begin with a brief overview of the basic elements of section 8 law. Next, I chronologically survey the Supreme Court's existing "digital section 8" jurisprudence; that is, each decision that has addressed allegations that the state has violated section 8 in a digital realm. The third part distils three key doctrines from these cases that are likely to animate future digital section 8 decisions: (i) the notion that "computers are different"; (ii) the role of contract, statute, and other exogenous norms in shaping privacy expectations over information obtained or held by third parties; and (iii) the application of the "biographical core" test to "low resolution" private information. While there is consensus as to the core meanings of each of these doctrines, to varying degrees each suffers from indeterminacy in application. I therefore propose refinements to minimize that indeterminacy. The fourth part examines, from both descriptive and prescriptive perspectives, how these doctrines played out in the Court's most recent digital section 8 decision: *R. v. Spencer*.[11] As always, the final part concludes.

II. SECTION 8 IN A NUTSHELL

Section 8's basic interpretive architecture is well settled. To establish a violation, claimants must demonstrate: first, that a governmental act constituted a "search or seizure"; and second, that the search or seizure was "unreasonable".[12]

The "search or seizure" question reduces to whether the act intruded on the claimant's "reasonable expectation of privacy".[13] If not, there was no "search or seizure" and no violation of section 8.[14] Accordingly,

---

[11] [2011] S.J. No. 729, 2011 SKCA 144 (Sask. C.A.) [hereinafter "*Spencer*"], affd [2014] S.C.J. No. 43, 2014 SCC 43 (S.C.C.) [hereinafter "*Spencer SCC*"].

[12] See generally Steven Penney, Vincenzo Rondinelli & James Stribopoulos, *Criminal Procedure in Canada* (Markham, ON: LexisNexis Canada, 2011), at para. 3.25 [hereinafter "Penney, Rondinelli & Stribopoulos"].

[13] *Hunter v. Southam Inc*., [1984] S.C.J. No. 36, [1984] 2 S.C.R. 145, at 159 (S.C.C.); *R. v. Dyment*, [1988] S.C.J. No. 82, [1988] 2 S.C.R. 417, at 426 (S.C.C.) hereinafter "*Dyment*"].

[14] See *R. v. Evans*, [1996] S.C.J. No. 1, [1996] 1 S.C.R. 8, at para. 11 (S.C.C.), *per* Sopinka J. [hereinafter "*Evans*"]; *R. v. Wise*, [1992] S.C.J. No. 16, [1992] 1 S.C.R. 527, at 533 (S.C.C.) [hereinafter "*Wise*"]; *R. v. M. (A.)*, [2008] S.C.J. No. 19, [2008] 1 S.C.R. 569, at para. 8 (S.C.C.), *per* Binnie J. [hereinafter "*A.M.*"].

absent any limits imposed by statute or other Charter provisions, the investigative technique comprising the act may be used without legal restriction, assuming similar factual circumstances.[15]

If, in contrast, the technique does invade a reasonable expectation of privacy, courts can regulate its use under section 8. Specifically, to be considered a "reasonable" search, courts may demand that the state actor conducting it meet certain conditions, such as obtaining a warrant based on probable grounds.[16] At a minimum, intrusions on reasonable expectations of privacy must be "authorized by law"; in other words, police must have a specific power to use the technique granted to them by legislation or common law.[17]

III. THE JURISPRUDENCE

1. *R. v. Plant*

The first digital search case to reach the Supreme Court of Canada was *R. v. Plant*, decided in 1993.[18] Police received an anonymous tip that a residence was being used to grow marijuana. Acting under a pre-existing arrangement with the local electricity provider, they accessed its customer database and discovered that the home was using four times more electricity than others of its size. Armed with this and other incriminating information, they obtained a warrant to search the home and seized marijuana.

The homeowner argued that by obtaining his electrical consumption records, police invaded his reasonable expectation of privacy without legal authority and therefore violated section 8 of the Charter. The Court disagreed, holding that the information obtained was not sufficiently

---

[15] See generally, *R. v. Duarte*, [1990] S.C.J. No. 2, [1990] 1 S.C.R. 30, at 42 (S.C.C.) [hereinafter "*Duarte*"]; *R. v. Wong*, [1990] S.C.J. No. 118, [1990] 3 S.C.R. 36, at 47 (S.C.C.); *R. v. Gomboc*, [2010] S.C.J. No. 55, [2010] 3 S.C.R. 211, at para. 20 (S.C.C.), *per* Deschamps J.

[16] I use the "probable grounds" as shorthand for the standard that courts and legislatures have termed "reasonable and probable grounds" or "reasonable grounds". In some cases courts have permitted searches on the basis of a lower standard termed "reasonable suspicion". See Penney, Rondinelli & Stribopoulos, *supra*, note 12, at paras. 3.132-3.140.

[17] See *R. v. Collins*, [1987] S.C.J. No. 15, [1987] 1 S.C.R. 265, at 278 (S.C.C.); *R. v. Caslake*, [1998] S.C.J. No. 3, [1998] 1 S.C.R. 51, at paras. 10-12 (S.C.C.); *R. v. Cole*, [2012] S.C.J. No. 53, [2012] 3 S.C.R. 34, at para. 64 (S.C.C.) [hereinafter "*Cole*"].

[18] [1993] S.C.J. No. 97, [1993] 3 S.C.R. 281 (S.C.C.) [hereinafter "*Plant*"].

"personal and confidential" to attract a reasonable expectation of privacy.[19] Writing for the (6:1) majority, Sopinka J. elaborated as follows:

> In fostering the underlying values of dignity, integrity and autonomy, it is fitting that s. 8 of the Charter should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual. The computer records investigated in the case at bar while revealing the pattern of electricity consumption in the residence cannot reasonably be said to reveal intimate details of the appellant's life since electricity consumption reveals very little about the personal lifestyle or private decisions of the occupant of the residence.[20]

Justice Sopinka further noted that the relationship between Mr. Plant and the provider was not confidential, the records were kept for the utility's own commercial purposes, and there were no contractual terms prohibiting disclosure to police.[21] To obtain the information, he added, police did not have to intrude "into places ordinarily considered private".[22]

In her concurring opinion, McLachlin J. (as she then was) would have held that the records did attract a reasonable expectation of privacy.[23] For her, the records told much about "one's personal lifestyle, such as how many people lived in the house and what sort of activities were probably taking place there", including the fact that marijuana was being grown.[24] She also took issue with Sopinka J.'s conclusion that the search was non-intrusive. "Computers may contain a wealth of personal information," she argued, and the information they store "may be as private as any found in a dwelling house or hotel room."[25] Lastly, she downplayed the importance of the lack of any contractual prohibition on disclosure, stating that "the question is not so much whether the relationship is one of confidence, so much as whether the particular records disclose a reasonable expectation of confidence".[26]

---

[19] *Id.*, at 293.

[20] *Id.*, at 293-94.

[21] *Id.*, at 294.

[22] *Id*.

[23] Justice McLachlin concurred in the result because she found that there was sufficient evidence, apart from the electricity records, to support the issuance of the warrant. *Id.*, at 304.

[24] *Id.*, at 302-303.

[25] *Id.*, at 303-304.

[26] *Id.*, at 303.

2. *R. v. Morelli*

Apart from one very brief affirming decision,[27] the next section 8 digital privacy case did not arise until 2010, when the Court released *R. v. Morelli*.[28] The key issue there (whether police had sufficient grounds to obtain a warrant to search a suspect's personal computer for child pornography) is not relevant to this paper. It was not disputed that the suspect had a reasonable expectation of privacy in his computer's contents.[29] By 2010, it would have been shocking had even one judge concluded otherwise.[30]

The Court's divergent pronouncements about the consequences of digitization, however, are revealing. At the beginning of his majority reasons, Fish J. signalled that the Court was cognizant of the especial importance of privacy in the digital age:

> It is difficult to imagine a search more intrusive, extensive, or invasive of one's privacy than the search and seizure of a personal computer.
>
> First, police officers enter your home, take possession of your computer, and carry it off for examination in a place unknown and inaccessible to you. There, without supervision or constraint, they scour the entire contents of your hard drive: your emails sent and received; accompanying attachments; your personal notes and correspondence; your meetings and appointments; your medical and financial records; and all other saved documents that you have downloaded, copied, scanned, or created. The police scrutinize as well the electronic roadmap of your cybernetic

---

[27] *Smith v. Canada (Attorney General)*, [2001] S.C.J. No. 85, [2001] 3 S.C.R. 902 (S.C.C.), affg [2000] F.C.J. No. 174, 252 N.R. 172 (F.C.A.), affg CUB-44824 (UIC Umpire) (reasonable expectation of privacy not breached when government unemployment insurance commission obtained claimant's travel records from customs agency through "data-match" program).

[28] [2010] S.C.J. No. 8, [2010] 1 S.C.R. 253 (S.C.C.) [hereinafter "*Morelli*"].

[29] Because the issue was not in dispute, the Court did not explicitly state that personal computers carried a reasonable expectation of privacy. But as the Court stated in *Cole*, *supra*, note 17, at para. 1, *Morelli* "left no doubt" on the issue.

[30] Recall that in her concurring reasons in *Plant*, *supra*, note 18, at 303-304, McLachlin J. observed that computers may contain a great deal of personal information. Note as well that the Court has repeatedly referred to a 1972 government report on computer privacy. See Task Force on Privacy and Computers, *Privacy and Computers: A Report of a Task Force Established Jointly by Dept. of Communications/Dept. of Justice* (Ottawa: Information Canada, 1972); *R. v. Lyons*, [1984] S.C.J. No. 63, [1984] 2 S.C.R 633, at 688 (S.C.C.); *Dyment*, *supra*, note 13, at paras. 19, 21, 29; *Plant*, *id.*, at 292; *R. v. Law*, [2002] S.C.J. No. 10, [2002] 1 S.C.R. 227, at para. 16 (S.C.C.); *R. v. Tessling*, [2004] S.C.J. No. 63, [2004] 3 S.C.R. 432, at para. 23 (S.C.C.) [hereinafter "*Tessling*"]; *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, [2013] S.C.J. No. 62, 2013 SCC 62, at para. 21 (S.C.C.).

> peregrinations, where you have been and what you appear to have seen on the Internet — generally by design, but sometimes by accident.[31]

Justice Deschamps' dissenting opinion also began with a comment on the "tremendous changes" wrought by "[i]nternet and computer technologies".[32] But, rather than stressing digitization's threat to privacy, she emphasized its capacity to "facilitate the communication of information and the exchange of material of all kinds and forms, with both legal and illegal content, and in infinite quantities."[33] "No one can be unaware today", she added, "that these technologies have accelerated the proliferation of child pornography because they make it easier to produce, distribute and access material in partial anonymity".[34]

3. *R. v. Gomboc*

Also decided in 2010, *R. v. Gomboc*[35] was the sequel to *Plant*. As in *Plant*, police suspected that a home was being used as a grow-op and wished to measure its electricity consumption. But, instead of obtaining billing records from the provider, they asked it to install a digital recording ammeter ("DRA") on the power line connected to the house. The provider complied, placing the DRA outside the home's property line. Compared to the billing records in *Plant*, the DRA provided more detailed, hourly usage data that enabled police to make stronger correlations with the cyclical usage patterns typical of grow-ops.[36]

A majority of the Court found that the DRA did not invade the homeowner's reasonable expectation of privacy. It divided, however, on the reasons for this conclusion. For the plurality, Deschamps J. held that the case could not be distinguished from *Plant*. Though the DRA produced more fine-grained measurements, it did not reveal intimate details of household activities.[37] The fact that the information came from

---

31 *Morelli*, *supra*, note 28, at paras. 2-3.

32 *Id.*, at para. 114.

33 *Id*.

34 *Id*. (internal citation omitted).

35 [2010] S.C.J. No. 55, [2010] 3 S.C.R. 211 (S.C.C.) [hereinafter "*Gomboc*"].

36 *Id*., at paras. 5, 38. The officer who testified about DRAs stated that of approximately 400 cases where DRA data was used to obtain a search warrant, grow-op evidence was found in all but one. *Id*., at para. 69, Abella J., concurring. DRAs can also provide accurate consumption information when conventional metering has been manipulated to thwart criminal investigation and defraud the provider. See, *e.g.*, *R. v. Cheung*, [2005] S.J. No. 474, 2005 SKQB 283, at para. 6 (Sask. Q.B.).

37 *Gomboc*, *supra*, note 35, at paras. 7-15, 36-40.

a home (normally a realm of strong privacy expectation[38]) did not trump this fact.[39] In her view, the evidence established that "there was absolutely no reliable inference to be made concerning the occupants or their activities in the house besides the grow operation".[40] And while the criminal nature of concealed activity does in itself disqualify it from section 8's protections, she stressed, the focus of the inquiry is not the "nature or identity of the concealed items" but rather the "potential impact of the search on the person [or thing] being searched".[41]

Further, she noted, police access to electrical consumption data was permitted by the governing legislative regime. The relevant regulation allowed disclosure of customer information to police absent the customer's express request that it remain confidential (which the homeowner did not make).[42] Though this legislation was not "sufficient to erode the expectation of privacy", she concluded, it "weighed heavily against giving the asserted expectation of privacy constitutional recognition".[43] She was careful to state, however, that given the great diversity of information "generated in customer relationships" and given that such relationships "are often governed by contracts of adhesion", courts should exercise caution in deciding the constitutional effect of legislative disclosure clauses.[44]

Justice Abella agreed that there was no reasonable expectation of privacy. But she would have found otherwise but for the disclosure clause.[45] For her, any information from "inside the home" is "presumptively" protected by a reasonable expectation of privacy.[46] The fact that the information reliably predicted the presence of a grow-op was enough to demonstrate the DRA's invasiveness.[47] She took an even stronger view than Deschamps J., however, on the Regulation's effect on

---

[38] *Id*., at para. 45. See also *Evans*, *supra*, note 14; *R. v. Silveira*, [1995] S.C.J. No. 38, [1995] 2 S.C.R. 297 (S.C.C.); *R. v. Feeney*, [1997] S.C.J. No. 49, [1997] 2 S.C.R. 13 (S.C.C.);*Tessling*, *supra*, note 30; *R. v. Patrick*, [2009] S.C.J. No. 17, [2009] 1 S.C.R. 579 (S.C.C.) [hereinafter "*Patrick*"].

[39] *Gomboc*, *id.*, at para. 50.

[40] *Id*., at para. 7.

[41] *Id.*, at para. 39, quoting *Patrick*, *supra*, note 38, at para. 32.

[42] *Code of Conduct Regulation*, Alta. Reg. 160/2003, s. 10(3)(f): permitting disclosure of customer information "to a peace officer for the purpose of investigating an offence if the disclosure is not contrary to the express request of the customer".

[43] *Gomboc*, *supra*, note 35, at paras. 32-33.

[44] *Id.*, at para. 33.

[45] *Id.*, at paras. 82-95.

[46] *Id.*, at para. 80.

[47] *Id.*, at para. 81.

the homeowner's expectation of privacy. Because he had an "unrestricted ability" to control the release of information,[48] she concluded, any subjective expectation of privacy he may have had was not objectively reasonable.[49]

Having dissented in *Plant*, it is not surprising that McLachlin C.J.C. did the same in *Gomboc*. Writing with Fish J., she agreed with Abella J.'s assessment of the DRA's invasiveness.[50] In addition to reliably revealing the presence of a grow-up,[51] they asserted, it enabled predictions about other "probable activities taking place within a home",[52] including "whether anyone is home, the approximate time at which the occupants go to bed and wake up, and guesses as to particular appliances being used".[53] A surveillance technique need not be capable of making "conclusive determinations" of residential activity to trigger a reasonable expectation of privacy, they reasoned.[54] It is enough that it enables "informed *predictions*" conveying "useful private information to the police".[55] Unlike Abella J., however, they concluded that legislation did not extinguish the homeowner's reasonable expectation of privacy.[56] A reasonable person could not have been expected to know that the legislation existed, let alone that it would be interpreted to permit the release of detailed electrical consumption data.[57]

4. *R. v. Cole*

The Court's next digital section 8 decision was 2012's *R. v. Cole*.[58] There, it had to decide whether a teacher had a reasonable expectation of privacy in a computer issued to him by his employer. While conducting routine maintenance, a school technician discovered nude photographs of a student on the computer. The technician notified the principal, who instructed him to make copies of the photos. The principal seized the

---

48 *Id*., at para. 85.
49 *Id.*, at para. 95.
50 *Id.*, at paras. 105, 124, 129.
51 *Id.*, at para. 129.
52 *Id.*, at para. 128.
53 *Id*.
54 *Id.*, at para. 125.
55 *Id.*, at para. 124 (emphasis in original).
56 *Id.*, at paras. 138-142.
57 *Id*., at paras. 139-140. See also Lisa Austin, "Getting Past Privacy? Surveillance, the Charter, and the Rule of Law" (2012) 27 Can. J.L. & Soc'y 381, at 394.
58 *Supra*, note 17.

computer, school board technicians made copies of temporary Internet files found on it, and both the computer and the copied files were sent to the police. Police examined the material and conducted a further forensic search of the computer.

Writing for a unanimous Court on this issue, Fish J. noted that the robust expectation of privacy ordinarily attaching to computer data was tempered by a number of factors, including the board's announced ownership of the device and its contents, the teacher's lack of exclusive access or control, the school's publicized policy of monitoring usage, and its explicit warning that computer data was not private.[59]

The Court nonetheless concluded that the teacher maintained a reasonable expectation of privacy. That expectation did not prevent his employer from either inspecting the computer in the course of routine maintenance or, once the photographs were found, searching it for school safety reasons.[60] But it did require police to obtain a warrant before examining the computer and its data. Despite its ownership, policies, and warnings, Fish J. observed, the school allowed the teacher to use the computer for "personal purposes".[61] "[R]egardless of where they are found or to whom they belong", he continued, computers "used for personal purposes" reveal intimate information about financial, medical, and personal matters as well as people's "specific interests, likes, and propensities".[62] This is especially true, he wrote, of devices connected to the Internet.[63]

5. *R. v. Vu*

Most recently, the Court issued its decision in *R. v. Vu*.[64] There, it had to decide whether police could search computers and a cell phone found by police searching a residence under a warrant authorizing, among other things, a search for documents. Though the warrant did not specifically authorize any computer searches,[65] under conventional law this would not have been a problem. Warrants to search places (such as residences)

---

59 *Id*., at paras. 8, 15-17, 50, 55-56.
60 *Id*., at paras. 61-62.
61 *Id.*, at para. 54.
62 *Id.*, at para. 47, quoting in part *Morelli*, *supra*, note 28, at para. 105.
63 *Id*.
64 [2013] S.C.J. No. 60, 2013 SCC 60 (S.C.C.) [hereinafter "*Vu*"].
65 *Id.*, at para. 4.

for things (such as documents) do not normally need to specify the location or container in which those things may be found.[66]

The Court concluded, however, that computers and mobile phones[67] were not analogous to "cupboards or filing cabinets".[68] Highlighting contemporary computers' massive storage capacities and the great diversity of intimate information they contain, Cromwell J. held for a unanimous Court that section 8's reasonableness requirement mandates specific, prior authorization to search computers.[69] If police find a computer (presumably in plain view[70]) while executing a warrant without such an authorization, they may seize it if they reasonably believe it contains evidence related to an offence.[71] But they may not search it unless they first obtain a specific warrant to do so.[72]

The Court was not willing, however, to proclaim a general rule requiring issuing judges to impose conditions dictating how computer searches should be conducted to limit unnecessary privacy invasions.[73] Requiring such conditions, Cromwell J. reasoned, would "likely add significant complexity and practical difficulty".[74] Claimants can challenge the reasonableness of computer searches *ex post*, however, and the rules emerging from these decisions may guide police on how to limit searches in future cases.[75] After-the-fact review, he added, may also spur future courts to develop rules constraining computer searches *ex ante*.[76] Lastly, given the complexity of the issue and the rapid rate of

---

[66] *Id.*, at paras. 23, 39.

[67] Notably, the Court concluded that contemporary mobile phones were equivalent to computers in terms of their storage and other capacities. All references to computers were thus specifically defined to include mobile phones. *Id.*, at para. 38.

[68] *Id.*, at para. 24.

[69] *Id.*, at paras. 40-48.

[70] On the requirements of plain view seizures, see Penney, Rondinelli & Stribopoulos, *supra*, note 12, at paras. 3.220-3.227.

[71] *Vu*, *supra*, note 64, at para. 49.

[72] *Id*.

[73] *Id.*, at paras. 53-62.

[74] *Id.*, at paras. 57-58 (noting the difficulty that U.S. courts have had in developing a consensus on how computer searches should be restrained *ex ante*).

[75] *Id.*, at para. 55.

[76] *Id*. Given that the Court was itself unwilling to proclaim any such rules, this statement is somewhat perplexing. Perhaps it is best understood as expressing an unwillingness, given the evidence on the record, to impose general, *ex ante* rules at the present time. But Cromwell J. did appear to contemplate the gradual imposition of such rules over time. See *id.*, at para. 62: "I would not foreclose the possibility that our developing understanding of computer searches and changes in technology may make it appropriate to impose search protocols in a broader range of cases in the future. Without expressing any firm opinion on these points, it is conceivable that proceeding in this

technological innovation, he suggested that Parliament might wish to intervene to tackle the issue "more comprehensively".[77]

IV. KEY DOCTRINES

Three key doctrines can be discerned in the cases that are likely to provide the foundation for future digital privacy decisions.

1. Computers Are Different

The first and most elemental doctrine, illustrated by *Morelli* and *Vu*, is that computers are "different"; in other words, the capacities of digital devices differ, often by several orders of magnitude, from their non-digital counterparts.[78] Simply put, computers typically contain both a vastly greater *quantity* and a vastly greater *variety* of personal information than their analogue counterparts. For example, digital devices often contain extensive records of communications content (text messages, e-mail and the like). Though non-digital "information containers" (such as briefcases, filing cabinets and notebooks) may contain personal communications (such as letters, calendars, and diary entries), the volume and diversity of information they hold is in no way comparable to that found on digital devices.[79] Indeed, the magnitude of communications content that may be extracted from digital devices may in some cases exceed that obtained through prospective communications

way may be appropriate in some circumstances." Note, as well, that issuing judges are required to impose conditions on the execution of searches on a case-by-case basis when necessary to ensure reasonableness under s. 8. See generally *Baron v. Canada*, [1993] S.C.J. No. 6, [1993] 1 S.C.R. 416 (S.C.C.); *Descôteaux v. Mierzwinski*, [1982] S.C.J. No. 43, [1982] 1 S.C.R. 860 (S.C.C.). Alluding to this requirement, Cromwell J. suggested in *Vu* that in some cases "authorizing justices may find it practical to impose conditions when police first request authorization to search. In others, they might prefer a two-stage approach where they would first issue a warrant authorizing the seizure of a computer and then have police return for an additional authorization to search the seized device." *Id.*, at para. 62.

[77] *Vu*, *id.*, at para. 56.

[78] See Daniel M. Scanlan, "Issues in Digital Evidence and Privacy: Enhanced Expectations of Privacy and Appellate Lag Times" (2012) 16 Can. Crim. L. Rev. 301, at 307-308 [hereinafter "Scanlan"].

[79] *Id*., at 308. See also *R. v. Fearon*, [2013] O.J. No. 704, 2013 ONCA 106, at para. 61 (Ont. C.A.), appeal heard and reserved May 23, 2014, [2013] S.C.C.A. No. 141 (S.C.C.): observing that mobile phones are "sophisticated devices which have a capacity for storing an infinite variety and amount of personal information in which there is a high expectation of privacy by the owner".

surveillance (*i.e.*, wiretaps),[80] which can only be conducted under onerous conditions exceeding those applicable to "ordinary" search warrants.[81]

That said, as discussed below in relation to the *Spencer* case, it can be dangerous to ascribe capacities to digital search technologies that they do not in fact possess. Judges must strive to understand the actual capacities of the privacy-invasive technologies before them, not speculative or theoretical capacities stemming from hype, misinformation or fear.[82]

2. Third Party Information and Extrinsic Norms

The starting point for this doctrine, exemplified by *Plant* and *Gomboc*, is the principle that reasonable privacy expectations may survive the disclosure of personal information to third parties. For those steeped in section 8 law, this proposition is neither novel nor controversial. But it is far from self-evident. In the United States, the so-called "third party doctrine" dictates that there is no reasonable expectation of privacy in information voluntarily or necessarily given to others, regardless of its inherent sensitivity or any conditions on disclosure imposed or expected by the subject.[83] As a consequence, vast troves of personal information (increasingly held in searchable, digital form) receive no constitutional protection.[84]

Presciently, the Supreme Court of Canada rejected this doctrine at an early stage of its section 8 jurisprudence. In *Plant*, Sopinka and

---

[80] See Scanlan, *id.*, at 308.

[81] *Criminal Code*, Part VI. See generally Steven Penney, "Updating Canada's Communications Surveillance Laws: Privacy and Security in the Digital Age" (2008) 12 Can. Crim. L. Rev. 115, at 118-21.

[82] See generally Paul Ohm, "The Myth of the Superuser: Fear, Risk, and Harm Online" (2008) U.C. Davis L. Rev. 1327 (experts in digital and Internet technology often exaggerate risks of harm). See also Timothy Caulfield, "Biotechnology and the Popular Press: Hype and the Selling of Sciences" (2004) 22 Trends in Biotechnology 337 (exploring legal implications of media-generated hype surrounding genetic technologies).

[83] See *United States v. Miller*, 425 U.S. 435 (1976) (banking records); *Smith v. Maryland*, 442 U.S. 735 (1979) (telephone records). See also *United States v. White*, 401 U.S. 745 (1971) (plurality) (no expectation of privacy when defendant communicates with informant surreptitiously carrying a "wire" transmitting conversations to police). Recently, however, some members of the Court have questioned the wisdom of retaining this doctrine in the digital era. See *United States v. Jones*, 132 S. Ct. 949 (2012), Sotomayor J.

[84] See Christopher Slobogin, *Privacy at Risk: The New Government Surveillance and the Fourth Amendment* (Chicago: University of Chicago Press, 2007), at 151-64; Susan W. Brenner & Leo L. Clarke, "Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data" (2006) 14 J.L. & Pol'y 211.

McLachlin JJ. both quoted from *Dyment*,[85] where La Forest J. opined that that "situations abound where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be protected".[86] In other words, though a person may impart confidential information to another for particular, instrumental reasons, the state should not be wholly free to conscript that information for its own purposes.[87]

This principle becomes especially important as more and more personal information is digitized, recorded, and stored in myriad searchable databases. Without some assurance that at least some of this information is protected from disclosure to government, people may lose trust in institutions and relationships, refrain from socially beneficial (but potentially stigmatizing) communications or activities, or deploy wasteful non-legal mechanisms to protect their privacy.[88]

But while a third party's possession of personal information does not preclude Charter protection, the nature of the relationship between the parties (including any governing contractual or legislative norms) may diminish or even extinguish privacy expectations. In *Plant*, for example, Sopinka J. noted that the commercial nature of the data and the lack of contractual terms restricting disclosure militated against section 8 protection.[89] Likewise in *Gomboc*, Abella J. (and to a lesser extent Deschamps J.) pointed to the legislative default disclosure rule in concluding that the claimant's expectation of privacy was unreasonable. In *Cole*, in contrast, the Court held that given the sensitivity of the

---

[85] *Dyment*, *supra*, note 13, at 429-30.

[86] See generally *Duarte*, *supra*, note 15 (reasonable expectation that private conversations not intercepted or recorded by state, even if one party aware of surveillance); *Cole*, *supra*, note 17, at paras. 67-73.

[87] See *Dyment*, *supra*, note 13, at 431-32 (reasonable expectation of privacy retained for bodily samples taken by medical personnel); *R. v. Colarusso*, [1994] S.C.J. No. 2, [1994] 1 S.C.R. 20, at para. 70 (S.C.C.) (blood samples held by coroner); *R. v. O'Connor*, [1995] S.C.J. No. 98, [1995] 4 S.C.R. 411, at para. 99 (S.C.C.) (records held by counsellors); *Lavallee, Rackel & Heintz v. Canada (Attorney General); White, Ottenheimer & Baker v. Canada (Attorney General); R. v. Fink*, [2002] S.C.J. No. 61, [2002] 3 S.C.R. 209, at para. 35 (S.C.C.) (records held by lawyers); *R. v. Dersch*, [1993] S.C.J. No. 116, [1993] 3 S.C.R. 768, at 778 (S.C.C.) (records held by physicians).

[88] See *Dyment*, *supra*, note 13, at 433-34. For more detailed versions of this argument, see Steven Penney, "Reasonable Expectations of Privacy and Novel Search Technologies: An Economic Approach" (2007) 97 J. Crim. L. & Criminology 477 [hereinafter "Penney, 'Novel Search Technologies'"]; Steven Penney, "Conceptions of Privacy: A Comment on *R. v. Kang-Brown* and *R. v. A.M.*" (2008) 46 Alta. L. Rev. 203; Tracey M. Bailey & Steven Penney, "Healing not Squealing: Recent Amendments to Alberta's *Health Information Act*" (2007) 15 Health L. Rev. 3, at 8 [hereinafter "Bailey & Penney"].

[89] *Supra*, note 18.

information at issue and the school board's acquiescence to personal use of its computers, the board's ownership and regulation of the claimant's computer data did not wholly defeat his privacy interest.[90]

Though these cases can be distinguished from one another, an emerging consensus can be distilled. To begin, section 8 sets out normative limitations on state power; its scope cannot therefore be (entirely) dictated by exogenous norms like statute or contract. As Deschamps J. put it in *Gomboc*:

> [T]he fact that the person claiming an expectation of privacy in information ought to have known that the terms governing the relationship with the holder of that information allowed disclosure may not be determinative. Rather, the appropriate question is whether the information is the sort that society accepts should remain out of the state's hands because of what it reveals about the person involved, the reasons why it was collected, and the circumstances in which it was intended to be used.[91]

Second, statute and contract are less likely to extinguish expectations of privacy over information that is intrinsically intimate. As McLachlin C.J.C. and Fish J. stated in *Gomboc*, "legislation is only one factor that is to be considered when determining whether an expectation of privacy is objectively reasonable and it may be insufficient to negate an expectation of privacy that is otherwise particularly compelling".[92]

This is a sensible approach. Consider the consequences of failing to recognize a reasonable expectation of privacy in *Cole*. Employer-issued digital devices have become ubiquitous, and employees commonly use them for personal purposes. Unrestricted state access to data from such devices could have many pernicious consequences, such as dissuading

---

[90] *Supra*, note 17.

[91] *Gomboc*, *supra*, note 35, at para. 34. See also *Tessling*, *supra*, note 30, at para. 42: "Expectation of privacy is a normative rather than a descriptive standard"; *Patrick*, *supra*, note 38, at para. 14; *R. v. Wong*, [1990] S.C.J. No. 118, [1990] 3 S.C.R. 36, at 46 (S.C.C.): the fundamental question in s. 8 cases is "whether giving their sanction to the particular form of unauthorized surveillance in question would see the amount of privacy and freedom remaining to citizens diminished to a compass inconsistent with the aims of a free and open society"; Anthony Amsterdam, "Perspectives on the Fourth Amendment" (1974) 58 Minn. L. Rev. 349, at 402.

[92] *Gomboc*, *id.*, at para. 115. Of course, legislative provisions permitting such disclosures are themselves subject to scrutiny under s. 8. See generally, *id*., at para. 58, *per* Deschamps J. (noting that the legislation was not subject to a Charter challenge); *Royal Bank v. Welton*, [2009] O.J. No. 209, 306 D.L.R. (4th) 487 (Ont. C.A.), leave to appeal refused [2009] S.C.C.A. No. 111 (S.C.C.) (rejecting s. 8, Charter challenge of disclosure exceptions in private sector privacy legislation).

people from engaging in socially productive and personally fulfilling communications and activities and inducing them to adopt costly and wasteful measures to preserve their privacy.[93]

Equally important, the costs to law enforcement of recognizing a reasonable expectation of privacy in workplace devices are marginal. As the Court noted in *Cole*, employers retain considerable scope to monitor devices and investigate work-related wrongdoing.[94] When such monitoring or investigation uncovers clear evidence of criminal activity, police will normally have little trouble obtaining a warrant to seize this evidence or conduct further searches.

3. The Biographical Core Test and "Low Resolution" Information

This still leaves the question of how to judge whether information is so intrinsically intimate as to be presumptively deserving of constitutional protection. As discussed, in *Plant*, the Court set out the "biographical core" test to answer this question. Like so many broadly stated, pragmatically grounded legal standards, the test works well in most situations. Everyone would agree that information about people's sexual, religious and political preferences[95] is more deserving of protection than information about their allegiances to sports teams. Nor would many dispute that (all other things being equal) information about residential activity is more intimate than behaviour conducted in public spaces, like driving or shopping.[96]

But as *Plant* and *Gomboc* illustrate, jurists often disagree about how to characterize investigative techniques that reveal "low resolution" information. Standing alone, such information may reveal little about intimate activity. But by viewing it in conjunction with other data, police may be able to determine (or at least infer the existence of) more

---

[93] See Steven Penney, "Unreasonable Search and Seizure and Section 8 of the Charter: Cost-benefit Analysis in Constitutional Interpretation" in Errol Mendes & Stéphane Beaulac, eds., *Canadian Charter of Rights and Freedoms*, 5th ed. (Markham, ON: LexisNexis Canada, 2013) 751, at 755-57 [hereinafter "Penney, 'Cost-benefit'"].

[94] The Court declined to comment on the implications of its decision for the rights of employers to monitor computers issued to employees. *Cole*, *supra*, note 17, at para. 60.

[95] See *Patrick*, *supra*, note 38, at para. 30, *per* Binnie J. and at para. 76, *per* Abella J., concurring; *Gomboc*, *supra*, note 35, at para. 7, Deschamps J. and at para. 121, McLachlin C.J.C. and Fish J., dissenting.

[96] See, *e.g.*, *Wise*, *supra*, note 14 (weaker expectation of privacy in vehicles than residences).

sensitive behaviour.[97] The debate over this kind of information centres on two related points: (i) the nature of the probabilistic inferences that can be drawn from the information (*i.e.*, whether police can infer the presence of intimate activity with reasonable reliability); and (ii) the relative merits of brighter or dimmer lines demarcating protected from unprotected information (*e.g.*, whether all information about residential activity should be protected, even if it does not permit reliable inferences in the case at hand).[98]

Elsewhere, I have argued how these debates should have been resolved in *Plant*, *Gomboc* and other existing Supreme Court decisions.[99] Below, I discuss on how they played out in *Spencer*.

V. *R. v. Spencer*: Is There a Reasonable Expectation of Privacy in Subscriber Information?

1. Background

The issue in *Spencer*[100] was whether the "subscriber" information associated with electronic communications attracts a reasonable expectation of privacy. Police often need this information to obtain warrants to acquire electronic communications content or metadata.[101]

As in many of the cases on this question, in *Spencer*, police determined that someone using a particular Internet Protocol ("IP") address was trading child pornography online. Using a publicly available database, they traced the address to Shaw Communications, a major Internet service provider.[102] Police wrote to Shaw requesting the identity of the subscriber associated with that address, purportedly in accordance with section 7(3)(c.1)(ii) of the *Personal Information Protection and*

---

[97] See generally Orin S. Kerr, "The Mosiac Theory of the Fourth Amendment" (2012) 110 Mich. L. Rev. 311. For non-digital Supreme Court cases wrestling with this issue, see *Tessling*, *supra*, note 30. See also Penney, "Cost-benefit", *supra*, note 93, at 762-67.

[98] See also *Tessling*, *supra*, note 30, at para. 34.

[99] Penney, "Cost-benefit", *supra*, note 93.

[100] *Supra*, note 11.

[101] See Robert W. Hubbard, Susan Magotiaux & Xenia Proestos, "The Limits of Privacy: Police Access to Subscriber Information in Canada" (2002) 46 Crim. L.Q. 361, at 372-73 [hereinafter "Hubbard, Magotiaux & Proestos"].

[102] See also *R. v. Ward*, [2012] O.J. No. 4587, 2012 ONCA 660, at paras. 25-26 (Ont. C.A.) [hereinafter "*Ward*"].

Electronic Documents Act.[103] As have most providers in similar circumstances,[104] Shaw complied, disclosing the name and billing information of the appellant's sister. After using this information to obtain a search warrant, police discovered an extensive cache of child pornography on the appellant's computer. The appellant asserted that the warrantless disclosure of the subscriber information violated section 8 of the Charter. The Crown countered, and the trial court agreed, that the disclosure was not a search or seizure because the subscriber information did not attract a reasonable expectation of privacy.

Reflecting the divisions about this question in other courts,[105] in *Spencer*, the Saskatchewan Court of Appeal divided in three ways.[106]

---

[103] S.C. 2000, c. 5 [hereinafter "PIPEDA"] (stating that organizations may disclose personal information without consent if police have identified their "lawful authority to obtain the information and indicated that … the disclosure is requested for the purpose of enforcing any law of Canada …"). Some jurists have interpreted "lawful authority" as requiring police to have a warrant or other compulsive process to obtain personal information under this provision. See, *e.g.*, *Re C. (S.)*, [2006] O.J. No. 3754, 2006 ONCJ 343 (Ont. C.J.); *R. v. Mahmood*, [2008] O.J. No. 3922, 236 C.C.C. (3d) 3 (Ont. S.C.J.). Most courts have rightly rejected this argument, noting (among other things) that such an interpretation would make s. 7(3)(c) of the Act (which permits disclosure when compelled by subpoena, warrant or court order) redundant. See, *e.g.*, *R. v. Kwok*, [2008] O.J. No. 2414, at para. 32 (Ont. C.J.) [hereinafter "*Kwok*"]; *R. v. Brousseau*, [2010] O.J. No. 5793, 2010 ONSC 6753, at paras. 41-45 (Ont. S.C.J.); *R. v. McNeice*, [2010] B.C.J. No. 2131, 2010 BCSC 1544, at para. 43 (B.C.S.C.); *R. v. Trapp*, [2012] S.J. No. 778, [2012] 4 W.W.R. 648, at paras. 114-118 (Sask. C.A.), *per* Ottenbreit J.A. [hereinafter "*Trapp*"]. See also Suzanne Morin, "Updated: Business Disclosure of Personal Information to Law Enforcement Agencies: PIPEDA and the CNA Letter of Request Protocol", Privacy Pages: CBA National and Privacy Access Law Section Newsletter (November 2011), at 3-8, online: <http://www.cba.org/cba/newsletters-sections/pdf/2011-11-privacy1.pdf> [hereinafter "Morin"] (examining provision's legislative history).

[104] See Morin, *id.*; *Ward*, *supra*, note 102, at paras. 37-38; Andrea Slane, "Privacy and Civic Duty in *R. v. Ward*: The Right to Online Anonymity and the Charter-Compliant Scope of Voluntary Cooperation with Police Requests" (2013) 39 Queen's L.J. 301, at 303.

[105] To date, the only other provincial court of appeal to deal with the issue has been Ontario's, which ruled in *Ward*, *id.*, that the subscriber information associated with an IP address did not attract a reasonable expectation of privacy in the circumstances. Trial courts have split on the question, with most finding no expectation of privacy. For a sample of decisions finding no expectation of privacy in IP subscriber information, see *R. v. Friers*, [2008] O.J. No. 5646, 2008 ONCJ 740 (Ont. C.J.); *R. v. Wilson*, [2009] O.J. No. 1067 (Ont. S.C.J.); *R. v. McGarvie*, [2009] O.J. No. 6417 (Ont. C.J.); *R. v. McNeice*, [2010] B.C.J. No. 2131, 2010 BCSC 1544 (B.C.S.C.); *R. v. Brousseau*, [2010] O.J. No. 5793, 2010 ONSC 6753 (Ont. S.C.J.); *R. v. Vasic*, [2009] O.J. No. 1968 (Ont. S.C.J.). Decisions going the other way include *R. v. Cuttell*, [2009] O.J. No. 4053, 2009 ONCJ 471 (Ont. C.J.); *Kwok*, *supra*, note 103; and *Re C. (S.)*, *supra*, note 103. For decisions on other types of subscriber information, see, *e.g.*, *R. v. Hutchings*, [1996] B.C.J. No. 3060, 111 C.C.C. (3d) 215, at paras. 22-26 (B.C.C.A.) (declining to find a reasonable expectation of privacy in telephone numbers, but noting that there was no evidence that the suspect's number was unlisted); *R. v. Brown*, [2000] O.J. No. 1177, at para. 63 (Ont. S.C.J.) (no reasonable expectation of privacy in mobile phone subscriber records); *R. v. Pervez*, [2005] A.J. No. 708 (Alta. C.A.) (same); *R. v. Stucky*, [2006] O.J. No. 108, [2006] O.T.C. 30 (Ont. S.C.J.) (no reasonable expectation of privacy in identifying

Justices Caldwell and Cameron agreed that because of its potential to reveal detailed and intimate information about lifestyle and personal choices, subscriber information generally attracts a reasonable expectation of privacy.[107] But Caldwell J.A. (and not Cameron J.A.) found that this expectation was extinguished by Shaw's service agreements and privacy policy, which warn customers that Shaw may disclose personal information to law enforcement.[108] Justice Cameron would have found that there was a reasonable expectation of privacy, but held in any event that the disclosure was reasonable under section 487.014(1) of the *Criminal Code*.[109] Justice Ottenbreit, in contrast, rejected the notion that subscriber information was sufficiently intimate or revealing to attract a reasonable expectation of privacy. "The potential that the Disclosed Information might in this case eventually reveal much about the individual and the individual's activity ...", he reasoned, is "neither here nor there".[110]

The Supreme Court concluded that the subscriber information attracted a reasonable expectation of privacy, that statute and contract did

information of postal box customer); *R. v. James*, [2013] O.J. No. 3591 (Ont. S.C.J.) (no reasonable expectation of privacy in name and account number associated with suspicious financial transactions); *R. v. Siemens*, [2011] S.J. No. 406 (Sask. Prov. Ct.) (no reasonable expectation of privacy in name of driver who rented car). American courts have almost universally rejected the notion that there is a reasonable expectation of privacy in Internet subscriber information. See, *e.g.*, *United States v. Perrine*, 518 F.3d 1196, at 1204-1205 (10th Cir. Kan. 2008); *United States v. Bynum*, 604 F.3d 161, at 164-65 (4th Cir. 2010); *United States v. Stults*, 575 F.3d 834, at 842-43 (8th Cir. Neb. 2009).

[106] *Supra*, note 11. At the same that it decided *Spencer*, the Court released its decision in *Trapp*, *supra*, note 103, in which a differently constituted court split two ways in a similar case. As in *Spencer*, Cameron J.A. (Jackson J.A., concurring) held that the accused had a reasonable expectation of privacy but that the search was reasonable. The remaining judge in *Trapp*, Ottenbreit J.A., concluded as he did in *Spencer* that there was no such expectation.

[107] *Spencer*, *id*., at paras. 22-27, Caldwell J.A., para. 98, Cameron J.A. Justice Caldwell also noted at paras. 34-42 that disclosure was permitted under PIPEDA.

[108] *Id*.

[109] This conclusion, which Cameron J.A. elaborated more fully in *Trapp*, *supra*, note 103, is clearly incorrect and was rejected by the Supreme Court in *Spencer*, *id.*, at paras. 71-73. Section 487.014(1) simply states that, "[f]or greater certainty," police do not require a production order to "ask a person to voluntarily provide to the officer documents, data or information that the person is not prohibited by law from disclosing." Since the provision does not create a police *power* to obtain the data (but merely confirms the general principle that police may seek people's voluntary cooperation to obtain investigative information), and since it imposes no limits on police's ability to do so, it cannot be said to authorize the disclosure. So, if the information obtained attracted a reasonable expectation of privacy (and thus constituted a "search or seizure"), its disclosure to police was not authorized by law and accordingly cannot be "reasonable" under s. 8. See also *Ward*, *supra*, note 102, at para. 50: "With respect to the contrary opinion reached by the majority in *Trapp*, at para. 66, I do not read s. 487.014(1) as creating or extending any police search or seizure power."

[110] *Spencer*, *id*., at para. 110 (emphasis in original).

not extinguish this expectation, and that the police's acquisition of the information was unreasonable under section 8 because it was not authorized by law. Though the appeal was dismissed (because the Court ruled that the evidence should not be excluded under section 24(2) of the Charter), henceforth police will not be able to obtain subscriber information by request from service providers.

Spencer implicates each of the three digital section 8 doctrines discussed above: (1) the technological nature of the investigative technique; (2) the effect of contract and statute in shaping reasonable privacy expectations; and (3) the application of the "biographical core" test to a type of information that some consider highly intimate and others not. In the context of subscriber information requests, (1) is so intimately related to (3) that I discuss them together. I therefore begin with (2).

2. Contract and Statute

Echoing Deschamps J.'s view in *Gomboc*, Cromwell J. held for a unanimous Court that contractual and statutory norms "may be relevant to, but not necessarily determinative of whether there is a reasonable expectation of privacy".[111] Indeed, in *Spencer* he found that these norms had little value in determining the reasonableness of the appellant's expectation of privacy.[112] The relevant contractual provisions were "confusing and equivocal", he wrote, and the statutory framework was "not much more illuminating".[113] Ultimately, he concluded that by incorporating PIPEDA by reference, the contractual framework permitted non-consensual disclosures only when authorized by law, which simply begs the question of whether a police request for voluntary disclosure invades a reasonable expectation of privacy under section 8 of the Charter.[114] In this case at least, contract and statute led to a tautology.[115]

---

[111] *Spencer SCC*, *supra*, note 11, at para. 54.

[112] *Id.*, at para. 55: "[T]he relevant provisions provide little assistance in evaluating the reasonableness of Mr. Spencer's expectation of privacy."

[113] *Id.*, at para. 60.

[114] *Id*., at para. 65: "The overall impression created by these terms is that disclosure at the request of the police would be made only where required or permitted by law."

[115] See *id*., at para. 63 (characterizing the relevant PIPEDA provisions (discussed further, *infra*, at notes 117-120 and accompanying text) as involving an "essential circularity").

The Court's reluctance to put much weight on either statutory or contractual norms in deciding whether there was a reasonable expectation of privacy in subscriber information was amply warranted. Consider first the statutory context. As mentioned, PIPEDA permits (but does not require) the organizations it governs to disclose personal information to police for law enforcement purposes. Both Caldwell J.A. in *Spencer*[116] and Doherty J.A. in *Ward*[117] found this to militate against finding a reasonable expectation of privacy. As discussed, however, section 8 guarantees a realm of privacy protection as against the state irrespective of state efforts to circumscribe privacy.[118] It is difficult to reconcile this "normative" conception of section 8 with one that permits privacy expectations to be diminished by statute.

It also makes little sense to read PIPEDA, which was designed to enhance individual privacy *vis-à-vis* non-state entities, as restricting individual privacy *vis-à-vis* the state.[119] Before PIPEDA and its provincial counterparts were enacted, police were free to request personal information from third parties, and absent legal process compelling disclosure (like a warrant), third parties were generally free to decide whether to comply. PIPEDA has not changed this. The law enforcement exemptions in PIPEDA and its analogues should not therefore be interpreted as militating either for or against recognizing a reasonable expectation of privacy.[120]

Contract presents a somewhat more difficult case. As noted by Doherty J.A. in *Ward*, to the extent that service agreements and privacy policies are binding, they are paradigmatically contracts of adhesion.[121] There is considerable diversity among providers and their privacy policies. But given the dominant market share of the largest few;[122] the uniformity of terms;[123]

---

[116] *Id*., at para. 41.

[117] *Ward*, *supra*, note 102, at paras. 100-104.

[118] See discussion *supra*, note 91 and accompanying text See also *Spencer*, *supra*, note 11, at para. 18.

[119] See *contra* Teresa Scassa, "Information Privacy in Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy" (2010) 7 Can. J. Law & Tech. 193, at 205 [hereinafter "Scassa"] ("If data protection legislation gives an open-ended discretion to companies to disclose personal information to police without the data subject's consent, and without need for judicial authorization, a person's reasonable expectation of privacy in this information would certainly seem to be diminished.").

[120] See Penney, Rondinelli & Stribopoulos, *supra*, note 12, at paras. 3.78-3.80; *R. v. Chehil*, [2009] N.S.J. No. 515, 248 C.C.C. (3d) 370 (N.S.C.A.), affd [2013] S.C.J. No. 49, [2013] 3 S.C.R. 220 (S.C.C.).

[121] *Ward*, *supra*, note 102, at paras. 52, 106. See also *Gomboc*, *supra*, note 35, at para. 33, Deschamps J.; *Spencer*, *supra*, note 11, at para. 54.

[122] See Canadian Radio-television and Telecommunications Commission, "Communications Monitoring Report 2013: Telecommunications service industry," § 5.3, online: <http://www.crtc.

and the length, complexity, and frequent amendment of those terms,[124] it is questionable whether consumers have much bargaining power with respect to their privacy.[125]

On the other hand, if consumers really do value the privacy of their subscriber information, the market would arguably respond accordingly.[126] On this view, the fact that the big providers permit disclosure speaks to the low value customers actually place on this aspect of their privacy.[127] Assuming a competitive marketplace and a reasonable measure of information symmetry,[128] consumers' acquiescence with these terms could plausibly count against recognizing a reasonable expectation of privacy in subscriber information.[129]

It is not clear which of these arguments is stronger. In the face of this uncertainty, the most sensible position may be to consider contractual terms, but be cautious before giving them much weight, especially when the information obtained is unequivocally intimate.[130] But in cases where the information is not especially sensitive (or is only debatably so), contractual terms clearly limiting privacy expectations may help sway the balance against section 8 protection, absent evidence of market failure.

3. Subscriber Information and the Biographical Core

Given the ambiguity and circularity of the statutory and contractual framework, the most critical determinant in *Spencer* was the Court's

---

gc.ca/eng/publications/reports/policymonitoring/2013/cmr5.htm> (the top five major Internet Service Providers captured 76 per cent of the market in 2012).

123 See Morin, *supra*, note 103, at 16-17 (compiling cases where courts have concluded that providers' customer agreements permit non-consensual disclosure of customer information to law enforcement) and 18-19 (finding such disclosure permitted under contemporary agreements).

124 See Scassa, *supra*, note 119, at 211.

125 See *Ward*, *supra*, note 102, at para. 106.

126 See Adam Thierer, "A Framework for Benefit-cost Analysis in Digital Privacy Debates" (2013) Geo. Mason L. Rev. 1055, at 1071-76 [hereinafter "Thierer"].

127 See Alessandro Acquisti, "The Economics of Personal Data and the Economics of Privacy: 30 Years after the OECD Privacy Guidelines", Paper #3 (December 2010) Organization for Economic Co-operation and Development, online: <http://www.oecd.org/sti/ieconomy/46968784.pdf> (surveying research showing willingness to disclose sensitive information for small rewards); Bettina Berendt, Oliver Günther and Sarah Spiekermann, "Privacy in e-commerce: Stated preferences vs. actual behavior" (2005) 48 Communications of the ACM 101 (experiment revealing divergence between privacy preferences and behaviour); Evelien van de Garde-Perik *et al.*, "Investigating Privacy Attitudes and Behavior in Relation to Personalization" (2008) 26 Social Sci. Computer Rev. 20, at 35-36, 39 (same).

128 See Thierer, *supra*, note 126, at 1071-72.

129 See *Ward*, *supra*, note 102.

130 See Scassa, *supra*, note 119, at 212.

measurement of the intrinsic intimacy of subscriber information, *i.e.*, whether it comprises part of the "biographical core" typically protected by section 8 of the Charter. On the face of it, it is difficult to see how a customer's name, address, or other identifying information (such as a telephone number, e-mail address or username) would reveal intimate details of people's lifestyles or personal choices, even if the information is not publicly available.[131] But police obviously did not want the subscriber information for its own sake. Rather, they wanted it to help discover the identity of the person downloading child pornography.[132]

The question then is whether piercing an Internet user's anonymity in these circumstances presents such a risk to privacy as to demand constitutional protection. The courts and commentators who have answered "yes" to this question have offered two major arguments. The first is that the *particular* information obtained by police, *i.e.*, the (likely) identity of a person observed to have accessed child pornography, revealed "intimate details of the lifestyle and personal choices of the individual".[133] The argument, in other words, is that use of child pornography is itself protected information, because it is an activity typically conducted in secrecy that people would not wish others to know about. The fact that possession and distribution of child pornography are criminal offences is immaterial: the activity is (almost by definition) intimate, so it deserves protection.

Perhaps surprisingly, the Supreme Court of Canada has sustained this argument, albeit in less emotionally fraught circumstances than child pornography.[134] As I have argued more extensively elsewhere, however, this principle is dubious.[135] There is an argument that courts should sometimes

---

[131] See Hubbard, Magotiaux & Proestos, *supra*, note 101, at 370-71, 373, 383-87. This is not to say that an individual's identity can never attract a reasonable expectation of privacy. In some circumstances, its disclosure may itself reveal intimate, personal information, such as the fact that a person has received medical treatment or legal advice. See Bailey & Penney, *supra*, note 88.

[132] See *Ward*, *supra*, note 102, at para. 68; *Spencer*, *supra*, note 11, at para. 19, Caldwell J.A.; Andrea Slane & Lisa M. Austin, "What's in a Name? Privacy and Citizenship in the Voluntary Disclosure of Subscriber Information in Online Child Exploitation Investigations" (2011) 57 Crim L.Q. 486, at 500-503.

[133] *Spencer*, *id.*, at para. 22, *per* Caldwell J.A.

[134] See *Gomboc*, *supra*, note 35, at paras. 7-15, 34-43, *per* Deschamps J.; paras. 80-82, *per* Abella J., concurring; and paras. 123-129, *per* McLachlin C.J.C. and Fish J., dissenting; *R. v. Kang-Brown*, [2008] S.C.J. No. 18, [2008] 1 S.C.R. 456, at para. 58 (S.C.C.), *per* Binnie J.; at para. 175, *per* Deschamps J., dissenting; and at para. 227, *per* Bastarache J., dissenting; *A.M.*, *supra*, note 14, at paras. 38, 67-73, *per* Binnie J.; and paras. 157-158, *per* Bastarache J., concurring; *Patrick*, *supra*, note 38, at para. 32.

[135] See Penney, "Novel Search Technologies", *supra*, note 88; Penney "Cost-benefit", *supra*, note 93, at 806-807.

use procedural law (like privacy rights) to constrain the enforcement of arguably unwise substantive offences.[136] But given the Supreme Court's pronouncements about the evils of child pornography offences (including simple possession),[137] this argument did not seem tenable in *Spencer*, and indeed, the Court did not advert to it.[138] Put bluntly, it sounds (and is in fact) perverse to interpret section 8 to protect subscriber information to preserve people's liberty to trade child pornography anonymously.

The second argument is more viable and was the one endorsed by the Court in *Spencer*. By obtaining Mr. Spencer's subscriber information, Cromwell J. suggested, police could potentially observe his online activity in a more sustained and general way. Though he was far from precise in detailing the nature of this potential surveillance, Cromwell J. concluded that any request for subscriber information that corresponds to "specifically observed, anonymous Internet activity engages a high level of informational privacy".[139]

Justice Cromwell is far from alone in fearing that subscriber information may give police access to reams of intimate information beyond the discovery of criminal activity. Many other jurists have made the same claim.[140] If this is true, unregulated police access to subscriber

---

[136] *Id*.

[137] See *R. v. Sharpe*, [2001] S.C.J. No. 3, [2001] 1 S.C.R. 45, at paras. 28, 82, 85-94 (S.C.C.) (recognizing significant risk that possession of child pornography increases the risk of child abuse).

[138] On this question, the Court stated only that the "nature of the privacy interest does not depend on whether, in the particular case, privacy shelters legal or illegal activity. ... [T]he issue is not whether Mr. Spencer had a legitimate privacy interest in concealing his use of the Internet for the purpose of accessing child pornography, but whether people generally have a privacy interest in subscriber information with respect to computers which they use in their home for private purposes…". *Spencer SCC*, *supra*, note 11, at para. 36. This statement simply reaffirms the uncontroversial principle that the discovery of illegality does not retrospectively justify intrusions that could have revealed intimate but legal activity. It does not support the idea, criticized above, that governmental intrusions revealing illegal activity should be regulated under s. 8, even if they are extremely unlikely to reveal intimate, legal activity.

[139] *Id*., at para. 51. See also *id.*, at para. 32: "The subject matter of the search was not simply a name and address of someone in a contractual relationship with Shaw. Rather, it was the identity of an Internet subscriber which corresponded to particular Internet usage."

[140] See *Spencer*, *supra*, note 11, at paras. 22-27, *per* Caldwell J.A.; Stanley A. Cohen, *Privacy, Crime and Terror: Legal Rights and Security in a Time of Peril* (Markham, ON: LexisNexis Canada, 2005), at 533; Slane, *supra*, note 104: Scassa, *supra*, note 119, at 218; Daphne Gilbert, Ian R. Kerr & Jena McGill, "The Medium and the Message: Personal Privacy and the Forced Marriage of Police and Telecommunications Providers" (2007) 51 Crim. L.Q. 469, at 487-89; Jennifer Stoddart, Privacy Commissioner of Canada, "Customer Name and Address (CNA) Information Consultation Document: Response of the Office of the Privacy Commissioner of Canada to Public Safety Canada" (October 2007) online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca/information/pub/lar_071108_e.pdf>, at 6.

information could indeed cause many of the privacy harms discussed above. But it is far from evident that this is correct. The evidence in *Spencer* and *Ward*, for example, showed that the subscriber information only allowed police to connect online activity with a likely user for brief, discrete periods of time.[141] This linking gave police access very little additional information about that person's online activities.

Commentators have nevertheless suggested that subscriber information gives police the *capacity* to scour the Internet for detailed records of subscribers' online activities.[142] There is no evidence in the jurisprudence, however, that police have done this or have the ability to do so.[143] As the cases illustrate, when police discover child pornography trading online, they can easily determine both the IP addresses of the traders and the service providers who assigned those addresses. But even assuming that an IP address remains attached to a particular subscriber for a significant period of time,[144] there is no ready means of searching the Internet for any other activity associated with that address.

The strongest argument that can be made for protecting subscriber information under section 8, then, is that it may be theoretically possible to use that information to engage in broader, unregulated surveillance of the subscriber's (undeniably intimate) online activities.[145] Since this possibility represents such a grave threat to privacy, the argument runs, courts should impose a bright line rule prohibiting unregulated access to subscriber information despite the fact that the information revealed in

---

[141] See *Ward*, *supra*, note 102, at para. 69: "I would say that the police sought information capable of putting the appellant at a specific place, at a specific time in the course of his travels on the Internet."

[142] See, *e.g.*, Mitch Koczerginski & Graham Mayeda, "They Promise They Won't Be Evil ... But Should Google Still Be Your Friend After *R v Ward*? (November 2013), online: <http://ssrn.com/abstract=2362933>.

[143] See *Ward*, *supra*, note 102, at para. 18: "[T]he evidence in this case does not support the contention that IP addresses are unique to individual subscribers or that combining an IP address with subscriber information allows the police to compile a history of a person's activity on the Internet. On this record, what is revealed is more in the nature of a snapshot than a history of one's Internet activity."

[144] In fact, in most cases users are assigned "dynamic" IP addresses that are reassigned after every connection to the Internet. See Joshua J. McIntyre, "Balancing Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should Be Protected As Personally Identifiable Information" (2011) 60 DePaul L. Rev. 895, at 900-902.

[145] See Office of the Privacy Commissioner of Canada, "What an IP Address Can Reveal About You" (May 2013), online: <https://www.priv.gc.ca/information/research-recherche/2013/ip_201305_e.pdf>.

the actual cases before them is mundane. Though not stated explicitly, this appears to be the rationale behind the Court's decision in *Spencer*.

The Court had previously rejected this kind of argument, however, in what is still the leading decision on the reasonable expectation of privacy question: *R. v. Tessling*. As Binnie J. stressed for a unanimous Court there, "the reasonableness line has to be determined by looking at the information generated by existing … technology, and then evaluating its impact on a reasonable privacy interest".[146] If the technology at issue changes, he added, "courts will have to deal with its privacy implications at that time in light of the facts as they then exist".[147]

Justice Binnie's reluctance to extrapolate from demonstrated existing technical capacity in *Tessling* was wise. As many commentators have noted, appellate courts are generally unsuited to the task of regulating complex and rapidly shifting technologies.[148] They deal with only that tiny fraction of uses of a technology that have been litigated to appeal (often years after the technology has been superseded); hear only the voices of advocates (including any interveners); and are largely limited to the evidentiary record developed at trial, with only very restricted capacities to engage with independent, technical expertise.[149]

All of this suggests that the Supreme Court may have been too eager to recognize a reasonable expectation of privacy in *Spencer*, especially if doing so would mean that police would need warrants to obtain subscriber information (even on reasonable suspicion). While police may have grounds to obtain such warrants in many cases (including on the facts of *Spencer*), in many others they may not. Police often need to obtain subscriber information attaching to computer modems/routers, mobile phones and other digital devices at very early stages of an investigation to develop leads, rule out suspects, ensure public safety and

---

146 *Supra*, note 30, at para. 29.

147 *Id*.

148 See Stephen Breyer, "Our Democratic Constitution" (2002) 77 N.Y.U. L. Rev. 245, at 261-63 [hereinafter "Breyer"]; Orin S. Kerr, "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution" (2004) 102 Mich. L. Rev. 801, at 875-76 [hereinafter "Kerr, 'Fourth Amendment'"]; see also Cass R. Sunstein & Adrian Vermeule, "Interpretations and Institutions" (2003) 101 Mich. L. Rev. 885; William J. Stuntz, "Accountable Policing" (Harvard Public Law Working Paper No. 130, 2006), online: <http://ssrn.com/abstract=886170>.

149 See Stuart Minor Benjamin, "Stepping Into the Same River Twice: Rapidly Changing Facts and the Appellate Process" (1999) 78 Tex. L. Rev. 269; Kerr, "Fourth Amendment", *id.*, at 875-76; Breyer, *id.*, at 261-63.

develop grounds to obtain search warrants or wiretap authorizations.[150] A warrant requirement would impede these efforts with little countervailing benefit to people's privacy.

Failing to recognize a reasonable expectation of privacy in *Spencer*, moreover, would not likely have opened the door to broader and more intrusive surveillance. First, section 8 of the Charter would likely apply to any governmental efforts to use subscriber information to systematically track online activities or conduct data mining with respect to identifiable persons.[151] As discussed, in *Spencer* and analogous cases police did not use subscriber information for these purposes. If reasonable privacy expectations are invaded by the state's acquisition of any information that might later be used for intrusive surveillance, almost any inquiry would trigger section 8 protection, severely hampering law enforcement.[152]

Second, if there is a need for systematic, prospective regulation of state access to subscriber records, Parliament is well placed to intervene. Compared to courts, legislatures are more directly responsive to people's preferences and can seek input from a much greater range of sources, including law enforcement, industry, advocacy groups, academics, technical experts and the general public.[153] And though the legislative process may sometimes be skewed (on the one hand, by the outsized influence of well-organized and deep-pocketed lobbies; and on the other, by the discounted influence of unpopular minorities),[154] there is little evidence that such bias has worked against the protection of online privacy.

---

[150] See Hubbard, Magotiaux & Proestos, *supra*, note 101, at 363, 372-73; Canadian Association of Chiefs of Police, "Simplifying Lawful Access — Bill C-30 — Through the Lens of Law Enforcement" (February 2012), online: <http://www.cacp.ca/media/library/download/1243/Final_Simplifying_Lawful_Access_final_english.pdf>, at 3-7, 14-15.

[151] See Wayne N. Renke, "Who Controls the Past Now Controls the Future: Counter-Terrorism, Data Mining and Privacy" (2006) 43 Alta. L. Rev. 779.

[152] See Steven Penney, "Updating Canada's Communications Surveillance Laws: Privacy and Security in the Digital Age" (2008) 12 Can. Crim. L. Rev. 115, at 154-58.

[153] See, *e.g.*, Department of Justice Canada, "Summary of Submissions to the Lawful Access Consultation" (April 28, 2003), online: <http://www.justice.gc.ca/eng/cons/la-al/sum-res/sum-res.pdf>.

[154] See generally Daniel A. Farber & Philip P. Frickey, *Law and Public Choice: A Critical Introduction* (Chicago: University of Chicago Press, 1991); Maxwell L. Stearns, ed., *Public Choice and Public Law: Readings and Commentary* (Cincinnati: Anderson, 1997); John Hart Ely, *Democracy and Distrust: A Theory of Judicial Review* (Cambridge: Harvard University Press, 1980) [hereinafter "Ely"]; Rosalind Dixon, "The Supreme Court of Canada, Charter Dialogue, and Deference" (2009) 47 Osgoode Hall L.J. 235, at 257-66 [hereinafter "Dixon"]; Thomas W. Merrill, "Does Public Choice Theory Justify Judicial Activism After All?" (1997) 21 Harv. J.L. & Pub. Pol'y 219; Michael J. Klarman, "The Puzzling Resistance to Political Process Theory" (1991) 77 Va. L. Rev. 747, at 763-68; Cass R. Sunstein, ed., *Behavioral Law and Economics* (Cambridge: Cambridge University Press, 2000);

Many commentators have argued that legislatures protect the privacy and liberty interests of criminal suspects, who are disproportionately poor, mentally ill and members of racial minorities.[155] Courts may therefore be justified in using expansive constitutional interpretations to regulate police-citizen encounters,[156] especially the kinds of recurring, street-level interactions empirically associated with discriminatory profiling and other abuses.[157] But when a surveillance technology is perceived to threaten the privacy of broad or powerful segments of society, legislatures have often been responsive.[158] This is almost certainly the case with requests for subscriber information and many other Internet-related investigative tools. In recent years, the federal government (under both Liberal and Conservative regimes) has proposed several Bills that would have enhanced law enforcement's abilities to obtain information from the digital realm, including provisions to compel the production of subscriber information.[159] In each case vigorous

---

Neil K. Komesar, *Imperfect Alternatives: Choosing Institutions in Law, Economics, and Public Policy* (Chicago: University of Chicago Press, 1994); Frank B. Cross, "Institutions and Enforcement of the Bill of Rights" (2000) 85 Cornell L. Rev. 1529; Michael C. Dorf & Michael Isaacharff, "Can Process Theory Constrain Courts?" (2001) 72 U. Colo. L. Rev. 923.

[155] See Anthony G. Amsterdam, "Perspectives on the Fourth Amendment" (1974) 58 Minn. L. Rev. 349, at 378-79; 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 Mich. L. Rev. 505, at 553-56; Donald A. Dripps, "Criminal Procedure, Footnote Four, and the Theory of Public Choice; or, Why Don't Legislatures Give a Damn About the Rights of the Accused?" (1993) 44 Syracuse L. Rev. 1079; Don Stuart, "Time to Recodify Criminal Law and Rise above Law and Order Expediency: Lessons from the Manitoba Warriors Prosecution" (2000) 28 Man. L.J. 89.

[156] See Penney, "Novel Search Technologies", *supra*, note 88, at 509-11; Ely, *supra*, note 154, at 97 (describing Fourth Amendment as "harbinger of the Equal Protection Clause"); William Stuntz, "Privacy's Problem and the Law of Criminal Procedure" (1995) 93 Mich. L. Rev. 1016.

[157] See generally *R. v. Golden*, [2001] S.C.J. No. 81, [2001] 3 S.C.R. 679, at para. 85 (S.C.C.); *R. v. Landry*, [1986] S.C.J. No. 10, [1986] 1 S.C.R. 145, at 186 (S.C.C.), *per* La Forest J, dissenting; *R. v. Brown*, [2003] O.J. No. 1251, 64 O.R. (3d) 161 (Ont. C.A.); *R. v. Harris*, [2007] O.J. No. 3185, 87 O.R. (3d) 214, at para. 63 (Ont. C.A.); David M. Tanovich, *The Colour of Justice: Policing Race in Canada* (Toronto: Irwin Law, 2006); Sujit Choudhry, "Protecting Equality in the Face of Terror: Ethnic and Racial Profiling and s. 15 of the Charter" in Ronald J. Daniels, Patrick Macklem & Kent Roach, eds., *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill* (Toronto: University of Toronto Press, 2001) 367; Benjamin L. Berger, "Race and Erasure in *R. v. Mann*" (2004) 21 C.R. (6th) 58.

[158] See Kerr, "Fourth Amendment", *supra*, note 148, at 839-58; Penney, "Novel Search Technologies", *supra*, note 88, at 503-505; Craig Lerner, "Legislators as the 'American Criminal Class': Why Congress (Sometimes) Protects the Rights of Defendants" (2004) U. Ill. L. Rev. 599, at 613-18; James Stribopoulos, "In Search of Dialogue: The Supreme Court, Police Powers and the Charter" (2005) 31 Queen's L.J. 1, at 18-30.

[159] See Bill C-74, *Modernization of Investigative Techniques Act*, 1st Sess., 38th Parl., 2005, ss. 17-19; Bill C-46, *Investigative Powers for the 21st Century Act*, 2d Sess., 40th Parl., 2009; Bill C-47, *Technical Assistance for Law Enforcement in the 21st Century Act*, 2nd Sess., 40th Parl.,

lobbying by privacy groups helped to kill the proposals.[160] There does not seem to be a need, therefore, for courts to constitutionalize protection for subscriber information to correct defects in the majoritarian political process.

Thankfully, however, the *Spencer* Court did not foreclose the possibility of a legislative response that could restore law enforcement's capacity to obtain subscriber information without a warrant. Recall that to cohere with section 8, any intrusion on a reasonable privacy expectation (*i.e.*, a "search or seizure") must be "authorized" by statute or at common law. Since there was no statutory or common law authority to obtain the subscriber information in *Spencer*, the Court simply concluded that the search was not authorized by law and hence was unreasonable.[161] This leaves room for a "dialogical" response by Parliament that would regulate warrantless access to subscriber information.[162] The lawful access Bills mentioned above, for example, included audit, usage, reporting and record-keeping requirements that would have greatly limited the possibility of racial profiling[163] or systematic data mining.[164]

VI. CONCLUSION

The digital age is upon us, and the law of search and seizure and section 8 of the Charter must inevitably adapt. But meeting this challenge should not require a dramatic overhaul of the Supreme Court of Canada's

2009, ss. 16-23; Bill C-30, *Protecting Children from Internet Predators Act*, 1st Sess., 41st Parl., 2012, ss. 16-23. A similar Bill is currently before Parliament, but it contains no provisions with respect to subscriber records. See Bill C-13, *Protecting Canadians from Online Crime Act*, 2nd Sess., 41st Parl., 2013.

[160] See Jesse Brown, "Slacktivism defeats Lawful Access" *Maclean's* (September 21, 2011), online: <http://www.macleans.ca/society/technology/slacktivism-defeats-lawful-access/> (detailing the influence of a 70,000-person petition opposing the proposed legislation); Michael Geist, "Ottawa finds public no pushover on snooping law" *The Toronto Star* (October 30, 2006) E03.

[161] *Spencer SCC*, *supra*, note 11, at para. 5.

[162] See generally Dixon, *supra*, note 154; Kent Roach, *The Supreme Court on Trial: Judicial Activism or Democratic Dialogue* (Toronto: Irwin Law, 2001); 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 Osgoode Hall L.J. 75.

[163] On the potential for online profiling, see Jason M. Young, "Surfing While Muslim: Privacy, Freedom of Expression and the Unintended Consequences of Cybercrime Legislation: A Critical Analysis of the Council of Europe Convention on Cybercrime and the Canadian Lawful Access Proposal" (2004-2005) 7 Yale J. L. & Tech. 346.

[164] *Supra*, note 151.

existing digital section 8 jurisprudence. The Court has already recognized the distinctiveness of digital devices, stressed the importance of maintaining privacy in third party records, and exhibited a reluctance to erode the normative core of section 8 by reference to extrinsic norms. In future cases, however, it is hoped that in refining the meaning of "biographical core" information, the Court will rethink its position on the protection of purely criminal information, focus on the actual (and not speculative) capacities of digital search and surveillance technologies, and be cognizant of its own informational limitations in seeking to regulate complex and changing technologies.