PRIVACY IN THE AGE OF THE INTERNET: LAWFUL ACCESS PROVISIONS AND ACCESS TO ISP AND OSP SUBSCRIBER INFORMATION

GRAHAM MAYEDA*

Bill C-30 (the Protecting Children from Internet Predators Act*) and the* Protecting Canadians from Online Crime Act *are two recent attempts by the Canadian government to create incentives for Internet Service Providers (ISPs) and Online Service Providers (OSPs) to disclose the subscriber information of Internet users to government agencies. In this article, the author argues that while such provisions may not violate section 8 of the* Charter *based on current judicial interpretation, they ought to be found unconstitutional. To date, the Supreme Court of Canada's search and seizure jurisprudence uses a normative framework that does not distinguish between defining the right to privacy and justifying limitations to it. This approach is not consistent with that taken for other* Charter *rights. The recent decisions of the Supreme Court in* R v. Spencer *and* R v. Fearon *may signal a slight shift, but they do not go far enough. If courts defined privacy interests more broadly than under current law and required the government to justify restrictions on these interests under section 1, this would create a legal regime that achieves a better balance between competing privacy and security interests.*

TABLE OF CONTENTS

* Graham Mayeda is an Associate Professor in the Faculty of Law at the University of Ottawa.

I. INTRODUCTION

People are increasingly aware of the threat that Internet use can pose to their privacy,[1] although many have only a vague understanding of its magnitude or nature.[2] One potential threat to privacy is the government and its agencies: governments have an interest in preventing the crimes that can be committed via cyberspace. Yet the means used to detect these crimes can often bring those not engaged in crime under undesirable government scrutiny as law enforcement agencies trawl for illegal online activities, catching the innocent in their nets.

The *Canadian Charter of Rights and Freedoms*[3] can notionally provide protection against such state action by requiring that government agents obtain judicially authorized search warrants or production orders before conducting a search. For instance, in *Hunter v. Southam Inc.*,[4] the seminal *Charter* case on what constitutes an unreasonable search under section 8, Justice Dickson held that warrantless searches of people, places and things in which the rights-holder has a reasonable expectation of privacy are presumptively unreasonable and hence a breach of the *Charter*.[5] When government actors restrict themselves to searches or seizures that have been approved by a judicial official, their behaviour is subject to court scrutiny, and by extension, public scrutiny. Where warrants are required, illegal searches can be prevented before they occur, as the court reviewing the application for a warrant or production order will require government agents to justify the search by explaining how the information already in their possession meets the requisite level of certainty set out by statute for the issuing of a warrant.[6]

---

1 Lee Rainie et al,"Anonymity, Privacy, and Security Online" (Washington, DC: Pew Research Center, 2013) at 4 (noting that 86 percent of internet users take steps to avoid surveillance); Government of Canada, *Canada's Cyber Security Strategy* (Ottawa: Government of Canada, 2010), online: <www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf> at 13–14; Curtis R Taylor, "Consumer Privacy and the Market for Customer Information" (2004) 35:1 RAND J Economics 631 at 632. In 2005, a survey conducted by CBS News found that 52 percent of Americans found their privacy was under "serious threat," while 30 percent thought that it was "already lost": Joel Roberts, "Poll: Privacy Rights Under Attack" *CBS News* (30 September 2005), online: <www.cbsnews.com/news/poll-privacy-rights-under-attack/>. In 2009, Turow et al found that a large majority of Americans disapprove of tailored advertising that depends on tracking their internet use: Joseph Turow, et al, "Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It," (Oakland: Rose Foundation for Communites and Environment, 2009), online: Social Sciences Research Network <ssrn.com/abstract=1478214>.

2 Patricia A Norberg, Daniel R Horne & David A Horne, "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors" (2007) 41:1 J Consumer Affairs 100 at 101 (referring to the "privacy paradox." The paradox is that people report that maintaining their privacy is important to them, and yet they make choices that demonstrate a remarkable lack of concern). See also Leslie K John, Alessandro Acquisti & George Loewenstein, "Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information" (2011) 37:5 J Consumer Research 858.

3 Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11 [*Charter*].

4 [1984] 2 SCR 145 [*Hunter*].

5 *Ibid* at 161.

6 For instance, a search warrant under the *Criminal Code*, RSC 1985, c C-46, s 487, requires that the police have reasonable grounds to believe that evidence of a crime is to be found at a particular place.

Government agencies and some academics have complained that Canada's warrant system is old and creaking — it is not up to the needs of modern, online life.[7] Steven Penney writes that these laws fail "to adequately protect against the novel threats to privacy posed by [new] technologies."[8] In consequence, the Canadian government introduced legislation to fix the old rules, the most recent examples being Bill C-30 (*Protecting Children from Internet Predators Act*)[9] and the *Protecting Canadians from Online Crime Act*,[10] which received royal assent in December 2014. Both pieces of legislation include "voluntary disclosure" provisions[11] — provisions that allow private telecommunications companies such as internet service providers (ISPs) and online service providers (OSPs) to voluntarily provide government agents with private information about their subscribers[12] that might be protected from such disclosure under federal or provincial privacy legislation.[13] These voluntary disclosure provisions do not require government actors to obtain a warrant or production order before making the request; all they need do is to find a company willing to disclose the information the government seeks.[14] To increase the likelihood that an ISP or an OSP would voluntarily disclose information, these laws create incentives (or remove disincentives such as legal liability for disclosure) for these companies to comply with government requests for subscriber information.

---

7 See e.g. *Canada's Cyber Security Strategy*, *supra* note 1 ("Canada's law enforcement agencies cannot combat trans-national cybercrimes with outdated investigative powers and tools" at 13). See also Steven Penney, "Updating Canada's Communications Surveillance Laws: Privacy and Security in the Digital Age" (2008) 12:2 Can Crim L Rev 115 at 116.

8 Penney, *ibid* at 116.

9 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 (first reading 14 February 2012) [Bill C-30]. This bill was abandoned.

10 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 [*Protecting Canadians from Online Crime Act*].

11 These provisions are more commonly called "lawful access" provisions because such laws make it lawful for state agents to access information in the hands of third parties. However, I will use the term "voluntary disclosure provisions" in this article for two reasons. First, they create incentives for service providers to disclose their clients' information. Second, they emphasize that such provisions do not necessarily comply with the Constitution. Lawful access provisions are "lawful" in the sense that the access is authorized by a properly-enacted law. But under the *Charter*, *supra* note 3, s 8, the law authorizing access might still be found unreasonable and hence a violation of constitutional protections against unreasonable search and seizure.

12 Bill C-30, *supra* note 9, cl 2, s 16 required that a person, including an ISP or OSP, provide information about subscribers, including name, address, telephone number, and e-mail address, upon written request by the RCMP, CSIS, the Commissioner of Competition, or any provincial police service. The *Protecting Canadians from Online Crime Act*, *supra* note 10, cl 20 amends the *Criminal Code*, *supra* note 6, s 487.0195, so that no person, including an ISP or OSP, would "incur any criminal or civil liability" for voluntarily disclosing information to a government agent that has requested it. This provision is meant to provide an incentive for ISPs and OSPs to disclose subscriber information: Michael Geist, "The Privacy Threats in Bill C-13, Part One: Immunity for Personal Info Disclosures Without a Warrant" (25 November 2013), *Michael Geist* (blog), online: <www.michaelgeist.ca/2013/11/c-13-privacy-threat-part-one/>.

13 Some Canadian cases have suggested that companies are authorized to disclose information about their customers even though it would otherwise be protected by federal privacy legislation such as the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 [*PIPEDA*] or its provincial equivalents. This is because such legislation authorizes the disclosure of customer information to a police service investigating the use of the company's services for acquiring or trading child pornography: see e.g. *R v Ward*, 2012 ONCA 660, 112 OR (3d) 321 at paras 99–105 [*Ward*]; *R v Trapp*, 2011 SKCA 143, 377 Sask R 246 at para 129 [*Trapp*]. Below, I discuss whether *R v Spencer*, 2014 SCC 43, [2014] 2 SCR 212 [*Spencer*], the most recent Supreme Court of Canada case on this topic, reverses this interpretation.

14 Bill C-30 was worded a bit more strongly than the *Protecting Canadians from Online Crime Act*. The latter merely creates incentives for ISPs or OSPs to provide information to government agencies by removing liability for doing so: *supra* note 10, cl 20. Bill C-30 used mandatory language, stating that "every telecommunications service provider must provide the person with identifying information in the service provider's possession or control": *supra* note 9, cl 2, s 16.

The overall question I address in this article is whether voluntary disclosure provisions are permitted under the *Charter*, and if so, whether they ought to be. Contrary to the views of others, I argue that voluntary disclosure provisions are not necessarily incompatible with the constitutional protections as interpreted in case law, including the Supreme Court of Canada's most recent decisions, *Spencer*[15] and *R. v. Fearon*.[16] This is because these cases define too narrowly the kinds of information in which a person has a reasonable expectation of privacy. Courts allow many factors to narrow this expectation, including laws and regulations such as voluntary disclosure provisions, standard form contracts between consumers and service providers, and privacy and acceptable use policies provided to consumers and employees. The consequence is that police can conduct many searches without a warrant, thus restricting Internet privacy. I argue in this article that current judicial interpretation of section 8 is inconsistent with the kinds of privacy that Canadians expect and that are necessary for them to pursue the interests that a robust sphere of privacy enables.

This article has three main parts. Part I introduces the reader to the overall structure of the paper. In Part II, I analyze legal rules such as those proposed in Bill C-30 and the *Protecting Canadians from Online Crime Act* that permit ISPs and OSPs to voluntarily disclose private information to government agencies. I begin with a short discussion of the appropriate normative framework within which ISPs, OSPs, and government ought to operate. While consent-based theories of privacy are the most common paradigm, I agree with Lisa Austin that it can be useful to analyze breaches of privacy in terms of rule of law values rather than breaches of personal autonomy that underlie the consent model. I then turn to the main argument, in which I explain the danger inherent in voluntary disclosure provisions and assess their constitutionality. In my view, provisions providing for voluntary disclosure without a search warrant are not necessarily unconstitutional. However, they are not likely to protect a level of privacy that is commensurate with public expectations, nor do they provide the robust protection of privacy which I believe section 8 of the *Charter* ought to require. Voluntary disclosure provisions create incentives for private corporations to betray the privacy interests of their clients. Moreover, they undermine the system of prior judicial authorization that jurisprudence interpreting section 8 of the *Charter* requires. The consequences of these voluntary disclosure provisions can be so corrosive of privacy interests protected by the *Charter* that they *ought* to be unconstitutional. However, what *ought* to be unconstitutional and what *is* unconstitutional under current interpretations of the *Charter* are often two different things. Thus, however reluctantly, I explain how these provisions are potentially justifiable under current Supreme Court of Canada jurisprudence.

In Part III, I fit my evaluation of voluntary disclosure provisions into the larger legal context of section 8 jurisprudence. I examine whether the case law analyzes privacy in a way that is defensible under a proper understanding of the Constitution and conclude that it does not do so. To justify this argument, I review why Canadian law has so far failed to provide an adequate normative framework for privacy. The section 8 case law has historically taken a sort of intuitive social welfare approach to breaches of privacy, protecting privacy up until the point where to protect it further would infringe other societal interests that the Supreme

---

15 *Supra* note 13.
16 2014 SCC 77, [2014] 3 SCR 621 [*Fearon*].

Court of Canada believes outweigh the protection of privacy.[17] The Court labels this intuitive approach a "normative" one.[18] However, the approach is not a true social welfare approach, because courts do not determine what the optimal level of privacy protection is on welfare grounds, nor do they hear evidence relevant to this issue. The Court's approach is also not normatively coherent. Judicial approaches to privacy encompass a variety of interests, including the protection of property, bodily integrity, control of information and, most recently, anonymity.[19] These multiple interests are not capable of being unified conceptually.[20] And while I do not believe that a single definition of "privacy" is possible,[21] courts should provide a way for gauging what is broadly considered "private" in Canadian social life.

A better approach to section 8 would be to define privacy interests broadly so that they accord with public notions of the private, but limit searches and seizures that invade privacy under section 1 of the *Charter* if protecting it has intolerable negative effects.[22] This balancing should be a nuanced, reasoned, and evidence-based process. Countervailing state interests should not be used to shrink the sphere of a person's privacy as the courts' approach to section 8 allows. Instead, once a broad privacy interest in information, such as subscriber information, has been established, courts should rigorously assess the proportionality of the individual's privacy interest in relation to the competing state interest. This process — in technical terms, leaving the balancing of competing rights to an *Oakes*[23] analysis under section 1 of the *Charter* — would ensure that courts publicly engage with important conflicting rights and interests, and fully explain in a public judgment why they believe the balance struck by the government is appropriate or not.[24] Such an approach promotes values underlying the rule of law such as accountability, publicity, and legitimacy.

II. VOLUNTARY DISCLOSURE PROVISIONS: UNDESIRABLE? YES; BUT UNCONSTITUTIONAL? PROBABLY NOT

In this part, I will evaluate the voluntary disclosure provisions in the *Protecting Canadians from Online Crime Act*. My conclusion is that such provisions are corrosive to our privacy

---

17 See e.g. Lisa M Austin, "Information Sharing and the 'Reasonable' Ambiguities of Section 8 of the Charter" (2007) 57:2 UTLJ 499 [Austin, "Information Sharing"].

18 *R v Tessling*, 2004 SCC 67, [2004] 3 SCR 432 at para 42 [*Tessling*], cited in *Spencer*, *supra* note 13 at para 18.

19 *Spencer*, *ibid* at para 41.

20 Elsewhere, I argue that the lack of a single unified concept of privacy is not a vice but a virtue. As an alternative to conceptual approaches, I present an emergent notion. See Graham Mayeda, "My Neighbour's Kid Just Bought a Drone … New Paradigms for Privacy Law in Canada" (2016) 35:1 NJCL 59.

21 Many privacy scholars have pointed to the different meanings of privacy in different contexts: see e.g. Daniel J Solove, *Understanding Privacy* (Cambridge, Mass: Harvard University Press, 2008) at 50.

22 A similar approach is taken to freedom of speech under section 2(b) of the *Charter*: see *Canadian Broadcasting Corp v Canada (Attorney General)*, 2011 SCC 2, [2011] 1 SCR 19 at para 34 [*CBC*].

23 *R v Oakes*, [1986] 1 SCR 103 [*Oakes*].

24 True, the section 1 analysis may be less rigorous today that when it was first conceived by Justice Dickson in *Oakes*: Graham Mayeda, "Between Principle and Pragmatism: The Decline of Principled Reasoning in the Jurisprudence of the McLachlin Court" in Sanda Rodgers & Sheila McIntyre, eds, *The Supreme Court of Canada and Social Justice: Commitment, Retrenchment or Retreat* (Markham, Ont: LexisNexis Canada, 2010) 41 at 54. But at least formally, it requires the government to demonstrate it has a pressing interest to pursue when violating constitutional rights, that its measure is effective in promoting this interest, and that the negative effects for constitutional rights are balanced by the salutary benefits of the measure. For a discussion of what the *Oakes* test has become: see Sujit Choudhry, "So What Is the Real Legacy of *Oakes*? Two Decades of Proportionality Analysis under the Canadian *Charter*'s Section 1" (2006) 34 SCLR (2d) 501.

rights. To this end, I will first describe the normative framework within which ISPs and OSPs make their decisions. This is important because, as Lisa Austin, drawing on the work of Robert Post, notes, the various actors in the privacy context — private citizens, private corporations, and government agents — work within different normative spheres.[25] This may be because they have different notions of privacy, but it is also because they make decisions differently. A short review of how private actors such as ISPs and OSPs make decisions about privacy will help to evaluate the "threat" that proposed voluntary disclosure provisions pose to an individual's privacy. After all, it is these companies that will be asked to voluntarily disclose information, and so it is important to understand what factors they take into account when deciding whether to do so. An understanding of how such provisions will affect privacy rights will help determine how best to promote privacy through a legal and regulatory regime. It will also provide a basis for evaluating alternatives.

Having reviewed how ISPs and OSPs make their decisions, I next evaluate the voluntary disclosure provisions in the *Protecting Canadians from Online Crime Act*. I argue that, based on how firms make decisions about whether to comply with a government request for disclosure, the voluntary disclosure provisions are not likely to promote constitutionally protected notions of privacy. It is very difficult to predict how firms will behave when requested to voluntarily produce documents because their decision is dependent on how the responses of consumers and government to disclosure or non-disclosure will affect the firm's profits. This leads to a typical principal-agent problem — the consumer must depend on the ISP or OSP to voluntarily protect her subscriber information, but she does not have an effective means for disciplining the service provider if it voluntarily discloses this information in a harmful way. For this reason, the voluntary disclosure provisions in the *Act* are not likely to maximize welfare by achieving an optimal balance between privacy protection and security.

Third, I will evaluate whether the voluntary disclosure provisions in the *Protecting Canadians from Online Crime Act* comply with the *Charter*. While some critics argue that the provisions would be unconstitutional, especially after the Supreme Court of Canada's decision in *Spencer*, I argue that this may not be the case. The provisions could pass constitutional review depending on how broadly one reads *Spencer*. *Spencer* confirms the Court's earlier decisions that voluntary disclosure provisions are relevant to determining a person's reasonable expectation of privacy. While Justice Cromwell holds that section 7(3)(c.1) of *PIPEDA* does not negate this expectation in Spencer's case,[26] the court leaves open the possibility that voluntary disclosure provisions could be relevant to determining a reasonable expectation of privacy in the future. Second, *Spencer* is equivocal about whether a properly drafted contract between an ISP and an OSP can put a consumer on notice that the service provider will disclose subscriber information to the police if they request it. A service provider's privacy policies and user agreement could also diminish a user's expectation of privacy in this information. Thus, where the scope of a person's reasonable expectation of privacy is narrower than the privacy protected by privacy protection statutes such as *PIPEDA*

---

25 Lisa M Austin, "Lawful Access and the Discretion to Disclose" in Dieter Dörr & Russell L Weaver, eds, *Perspectives on Privacy: Increasing Regulation in the USA, Canada, Australia and European Countries* (Berlin: De Gruyter, 2014) 96 at 98–99 [Austin, "Lawful Access"].

26 *Spencer*, *supra* note 13 at para 61.

or its provincial equivalents,[27] voluntary disclosure provisions may facilitate state agents obtaining a consumer's subscriber information.[28]

A. VOLUNTARY DISCLOSURE PROVISIONS CREATE INCENTIVES FOR FIRMS TO VIOLATE PRIVACY INTERESTS THAT THEY HAVE A DUTY TO PROTECT

To describe how ISPs and OSPs are likely to make decisions to disclose or protect their clients' private information, I will use some analysis drawn from the law and economics literature. However, it is important to set this analysis in context. The scope of a law and economics analysis is limited: it analyzes how actors respond to particular incentives, but it does not address the normative question of how a private firm as a moral actor ought to behave. If we accept that corporations have social responsibilities, voluntarily disclosing private subscriber information to government agents is arguably a violation of them. Why? The usual paradigm for assessing the responsibilities of private actors to respect privacy interests is the "consent" paradigm — companies should only disclose clients' information with their consent.[29] To the extent that voluntary disclosure provisions encourage and facilitate disclosure without consent, they run afoul of this requirement.

However, the consent framework suffers from certain deficiencies as a justification for protecting privacy. Lisa Austin points to the growing literature criticizing it.[30] Among these criticisms is that it is hard to obtain truly informed consent from consumers, who are often unable to understand the real-life consequences of consenting to access of their private information.[31] Assessing these consequences is even more difficult when it is unclear to whom a corporation might disclose information. As Austin points out, corporations play an all-pervasive role in our social interactions; the consumer and corporation are not in an exclusive relationship. Rather, "these companies act as intermediaries between individuals and the state, complying with various types of requests and orders by state authorities for

---

27 See for example, in Alberta, the *Personal Information Protection Act*, SA 2003, c P-6.5 [*PIPA*]; in British Columbia, the *Personal Information Protection Act*, SBC 2003, c 63; and in Quebec, *An Act Respecting the Protection of Personal Information in the Private Sector*, CQLR c P-39.1. These Acts have been deemed to be "substantially similar" to *PIPEDA*, *supra* note 13, and apply to businesses operating wholly within the relevant province.

28 An example is *R v Orlandis-Habsburgo*, 2014 ONSC 3096, 311 CRR (2d) 245 [*Orlandis-Habsburgo*], in which the Ontario Superior Court held that, where there is no reasonable expectation of privacy in information, a provincial statute containing a voluntary disclosure provision authorized an electricity utility to disclose the accused's customer information to police investigating drug production and trafficking charges.

29 For a discussion of the consent paradigm: see Julie E Cohen, "Between Truth and Power" in Mireille Hildebrandt & Bib van den Berg, eds, *Freedom and Property of Information: The Philosophy of Law Meets the Philosophy of Technology* (New York: Routledge) [forthcoming 2016]. See also Lisa Austin's discussion of the shortcomings of this paradigm: Lisa M Austin, "Enough About Me: Why Privacy is About Power, not Consent (or Harm)" in Austin Sarat, ed, *A World Without Privacy: What Law Can and Should Do?* (Cambridge: Cambridge University Press, 2015) 131 [Austin, "Enough About Me"].

30 Austin, "Enough About Me," *ibid* at 136. Austin cites Alessandro Acquisti & Jens Grossklags, "What Can Behavioral Economics Teach Us About Privacy?" in Alessandro Acquisti et al, eds, *Digital Privacy: Theory, Technologies and Practices* (New York: Auerbach Publications, 2008); Daniel J Solove, "Privacy Self-Management and the Consent Dilemma," (2013) 126:7 Harv L Rev 1880; Fred H Cate, "The Failure of Fair Information Practices Principles," in Jane K Winn, ed, *Consumer Protection in the Age of the 'Information Economy'* (Burlington, Vt: Ashgate, 2006) 358 at 360. See also Austin, "Lawful Access," *supra* note 25 at 100.

31 See e.g. Solove, *ibid* at 1885–86.

information about their clients."[32] It is difficult for individuals to meaningfully assess the effects of disclosure of information to a corporation that is enmeshed in a web of relationships with third parties, both private and public.

As an alternative to the consent-based model, Austin proposes one based on relationships of power. This has two dimensions. First, she argues that one of the problems with breaches of privacy is that the actor that discloses the information has acted arbitrarily and abused its discretion.[33] She calls this the "power-over" problem, because a party with information about another holds power over her.[34] According to Austin, when one party holds power over another, the rule of law usually prohibits the powerful party from using that power arbitrarily.[35] If a company has power over an individual by virtue of holding private information about her, the rule of law requires that this power be controlled by legal principles such as transparency and accountability.[36]

The second dimension of Austin's power analysis, which she calls the "power-to" analysis, is that violations of privacy are problematic not just because they harm important interests, but because the failure to protect privacy denies individuals the ability to participate in certain kinds of activities that have personal and social benefit.[37] Privacy is necessary for people to have the power to pursue the kind of interests they are justified in choosing.[38] It follows from this that we have a responsibility to ensure that private corporations use the power they have over others wisely by virtue of possessing private information. Again, transparency and accountability are essential. But this time, the key is not what is disclosed and to whom, but how corporations use private information. The public ought to be aware of how uses of information by private corporations "prevent me from exercising some right in the future that might make me better off."[39] A legal framework protecting privacy is necessary in order to ensure that corporations in possession of private information protect it sufficiently for their customers to have the benefit of a justifiable sphere of privacy within which they can explore their identity and engage in worthwhile private activities.

In my view, Austin's "power-to" analysis is more fundamental than the "power-over" analysis. Humans require a sphere of privacy in order to explore dimensions of our identity or participate in activities that we are not yet prepared to engage in publicly. To secure this sphere, the law must exercise oversight over government and private sector actors — that is, the law must rein in their exercise of power over us, to use Austin's terminology — in order to facilitate and promote the worthwhile endeavours that individuals engage in privately, be it writing poetry or a novel, exploring sexual or gender identities, or engaging in debate about controversial ideas and issues.

---

32 Austin, "Enough About Me," *supra* note 29 at 140 (by "arbitrarily," she means that the corporation has made the decision without guidelines as to how to make a decision consistent with the public interest).
33 *Ibid* at 160–65.
34 *Ibid* at 160–61.
35 For a typical example of the problems with arbitrary uses of power, see Lon L Fuller, *The Morality of Law* (New Haven: Yale University Press, 1964).
36 Austin, "Enough About Me," *supra* note 29 at 164.
37 *Ibid* at 160–61.
38 *Ibid* (Austin says that privacy norms "secure our conditions of social interaction" at 177).
39 *Ibid* at 176.

Austin's analysis explains why private actors should not have unlimited power to interfere with our privacy interests — but it does not explain why these interests are important in the first place. Elsewhere, I have suggested that an "emergent" notion of privacy would fill the gap.[40] In my view, an explanation of why privacy is important must have a phenomenological (experiential) dimension rooted in concrete forms of social interaction. The line between the public and the private and the importance of the latter cannot be determined in advance based on a particular *idea* of privacy.[41] Instead, what privacy is and what its scope ought to be *emerge* from the constantly changing forms of social interaction that are prevalent in society. What is private and what is public is something we experience — social norms emerge from the way in which we interact in society; they are not the conceptual presuppositions of this interaction.

What do I mean when I say that the distinction between public and private "emerges" from social interaction? Take the example of *Spencer*. In that case, the Supreme Court of Canada recognized that the way in which we use the Internet requires the expansion of constitutionally-protected privacy interests to include online anonymity.[42] The Court thus recognizes the need for the law to protect an increasingly important dimension of social interaction whose promotion requires the protection of online anonymity — a new dimension of privacy. In *Fearon*, the Court limited police powers to search smartphones because of a recognition of how we use them today — they are essentially portable computers that contain a huge amount of personal, private data.[43] In each case, courts have expanded the sphere of constitutionally-protected privacy not by reasoning from a concept of privacy, but by recognizing the role that privacy plays in facilitating forms of social interaction that we value.

In the limited scope of this article, it is not possible to fully articulate this view. But it is important to acknowledge the limits of the economic analysis that is employed in the following sections. There, I will argue that a law is ineffective in protecting privacy if it does not create incentives for those who hold private information to act as responsible agents for those whose information they possess. I also suggest that where a law does not create incentives to protect privacy and this failure results in the infringement of constitutionally protected expectations of privacy, the law is incompatible with the Constitution. But this analysis does not address the normative question of whether these corporations have a moral responsibility to act in the public interest rather than solely in accordance with the private interests of their owners. In this section, I argued that they do have such a responsibility, and that it ought to be put into operation through holding them accountable for the disclosure of private information and making this disclosure transparent to those who provide information to ISPs and OSPs.

---

40 Mayeda, *supra* note 20.

41 Many privacy scholars acknowledge the importance of privacy for the promotion and protection of their idea of human identity. For instance, Thomas Nagel explains the "importance of concealment as a condition of civilization": Thomas Nagel, "Concealment and Exposure" (1998) 27:1 Philosophy & Public Affairs 3 at 4. Hamish Stewart explains that protection of privacy promotes three values, "authenticity, intimacy, and self-presentation," which are essential to a meaningful human existence: Hamish Stewart, "Normative Foundations for Reasonable Expectations of Privacy" (2011) 54 SCLR (2d) 335 at 355.

42 *Spencer*, *supra* note 13 at paras 34, 41–49.

43 *Fearon*, *supra* note 16 at paras 54, 58, Cromwell J; paras 100–102, Karakatsanis J, dissenting.

Having briefly touched on the proper normative framework within which corporations should make decisions about disclosing private information to government agents, I turn now to an economic analysis of the incentives created by voluntary disclosure provisions as an introduction to an analysis of why such provisions undermine privacy interests.

B. HOW ISPS AND OSPS MAKE DECISIONS AND THE CONSEQUENCES FOR AN APPROPRIATE REGULATORY REGIME

"Voluntary disclosure" provisions — laws that give ISPs and OSPs the discretion to disclose subscriber information to government officials — are unlikely to ensure adequate levels of privacy protection. To see why, we must understand how firms will behave when given complete freedom to disclose or not disclose subscriber information. This in turn requires us to examine the interests of firms, consumers, and government.

The behaviour of firms that collect private information about their customers is dependent on many variables, some of which may encourage a firm to infringe privacy. Private information can be useful to a firm by allowing it to determine that customer's consumer preferences, thus facilitating the tailoring of advertising of its products.[44] The information also allows the firm to develop better Internet traffic models,[45] thereby improving the efficiency of its services. It provides opportunities to enhance profits by offering goods at different prices to different consumers (price discrimination)[46] or by recommending particular products to consumers that are most likely to purchase them.[47] The value of this information creates an incentive for firms to collect private information and to share it within their various units. There are likewise incentives for firms to sell the information to third parties.[48] Some have even noted that social welfare can be increased by sharing information between two firms, as this can reduce market distortions.[49] For all these reasons, it is not surprising that firms are under tremendous pressure to share private information both within the firm and with third parties in ways that consumers did not anticipate when they provided it. Such behaviour may also infringe privacy laws, thus creating a tension between the public interest in privacy and the firm's profit-motivated self-interest.

As we can see, there are many incentives that lead firms to violate rather than protect their clients' privacy. These incentives often do not align with those of consumers, who use a

---

44 Alessandro Acquisti, "The Economics of Personal Data and the Economics of Privacy" (Background Paper #3 delivered at the Joint WPISP-WPIE Roundtable on the Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines, 1 December 2010) at para 31, online: OECD <http://www.oecd.org/sti/ieconomy/46968784.pdf> [Acquisti, "The Economics of Personal Data"]. He cites: Alessandro Acquisti & Hal R Varian, "Conditioning Prices on Purchase History" (2005) 24:3 Marketing Science 367; Robert C Blattberg & John Deighton, "Interactive Marketing: Exploiting the Age of Addressability" (1991) 33:1 John Sloan Management Rev 5.

45 Joan Feigenbaum et al, "Privacy Engineering for Digital Rights Management Systems" in Tomas Sander, ed, *Security and Privacy in Digital Rights Management* (Berlin: Springer, 2002) 86 at 88.

46 Acquisti, "The Economics of Personal Data," *supra* note 44 at para 32; Hal R Varian, "Price Discrimination and Social Welfare" (1985) 75:4 The American Economic Review 870.

47 Acquisti, "The Economics of Personal Data," *ibid*; James Bennett & Stan Lanning, "The Netflix Prize" (Paper delivered at the Knowledge Discovery and Data Mining Cup, 12 August 2007) [unpublished], online: University of Illinois Department of Computer Science <www.cs.uic.edu/~liub/KDD-cup-2007/proceedings/The-Netflix-Prize-Bennett.pdf>.

48 Acquisti, "The Economics of Personal Data," *ibid* at paras 16, 81.

49 *Ibid* at para 11, citing Giacomo Calzolari & Alessandro Pavan, "On the optimality of privacy in sequential contracting" (2006) 130:1 J Economic Theory 168.

different calculus.[50] As Ryan Calo explains,[51] when consumers seek to protect their privacy, they wish to avoid two basic kinds of harms — subjective harms, such as, emotional or psychological dissatisfaction resulting from the disclosure of private information;[52] and objective harms, such as, physical, psychological or economic harms that result from disclosure.[53] Without proper incentives to do so, firms such as ISPs or OSPs are unlikely to give as much protection to consumers' private information as consumers would like. As Alessandro Acquisti explains, there is a high risk of moral hazard — for example, the hazard that, in the absence of legal rules that create incentives for them to do otherwise, these companies will take risks with their clients' data.[54]

However, sometimes the interests of ISPs or OSPs and subscribers coincide. This occurs if the firm's reputation is very valuable to it, that is, if its clients prefer to deal with a company that will provide greater protection of their privacy, and the market is competitive enough to provide consumers with alternatives so that they can choose a firm that provides these protections. In this case, there may be an incentive for the firm to comply with privacy legislation, at least to the degree that the legislative goals mesh with consumer or client interests.[55] However, it is difficult to predict where the calculus of a firm's interests will lead, since it is highly dependent on the nature of its business and how privacy sensitive its consumers are,[56] as well as how competitive the market is.

Another factor to take into account when we assess how a legislative scheme will affect privacy is the effect of such a scheme on firm behaviour. Most legislators assume that legislation creates incentives for firms to act in a way that is more consistent with the public interest as embodied in the legislation. But the law and economics literature confounds this assumption. These scholars have long argued that it is difficult to create a set of legal rules that forces firms to internalize all the negative social costs of their behaviours: if the cost of

---

50 It is important to note that, even if the legal regime protected privacy in the way that consumers would prefer, this would not necessarily maximize social welfare. As law and economics scholars have long argued, protecting privacy may reduce social welfare by making it difficult or impossible for others to obtain the information they need to make the best allocation of their scarce resources: Richard A Posner, "Privacy, Secrecy, and Reputation" (1978) 28:1 Buff L Rev 1. The classic example is that firms can make better hiring decisions when potential applicants disclose all relevant information to them, but privacy laws and anti-discrimination laws often forbid employers from obtaining this information.

51 M Ryan Calo, "The Boundaries of Privacy Harm" (2011) 86:3 Ind LJ 1131.

52 *Ibid* (Calo describes such harms as "the perception of unwanted observation" at 1133).

53 *Ibid* (common examples include receiving unwanted spam, disclosure of private information to undercover intelligence agencies, or the unwanted taking of bodily substances).

54 Acquisti, "The Economics of Personal Data," *supra* note 44 at para 79.

55 The Office of the Privacy Commissioner suggests that this is one of the important motivations for firms to adhere to *PIPEDA*: see Office of the Privacy Commissioner of Canada, *Privacy Toolkit: A Guide for Businesses and Organizations* (Gatineau: Office of the Privacy Commissioner of Canada, 2014) at 1, online: <www.priv.gc.ca/information/pub/guide_org_e.pdf>. See also Feigenbaum et al, *supra* note 45 at 88.

56 Richard Epstein explains that "there is no independent public-regarding view": Richard A Epstein, "Deconstructing Privacy: And Putting It Back Together Again," (1999) John M Olin Law & Economics Working Paper No 75 (2d) at 20, online: University of Chicago Law School <www.law.uchicago.edu/files/files/75.Epstein.Privacy.pdf>. He uses this expression when talking about the right of an employee to keep certain information private from his or her employer. Usually, the personal life of an employee is of no value to the employer, and hence, the employer will be regarded as having no right to information about it. But "[l]et the employee receive comprehensive benefits from the employer, such as health care, and the calculus may well shift radically: now it does matter whether the employer drinks, smokes, or exercises on a regular basis" (*ibid* at 20). It is on this basis that Epstein makes his comment that there is no independent public-regarding view about the right to privacy of an employee in her personal information — it all depends on the nature of her relationship with the employer. Likewise, the "right to privacy" of an Internet user will likely be a function of the use to which a firm can put private information.

complying with the regulatory regime is too high — that is, if the benefits of breaking the law outweigh the costs of being found in breach of it — rational firms will not comply with the regime, instead preferring to breach their subscribers' privacy and internalize the costs of non-compliance.[57] In simple terms, it may be more profitable to sell more products by breaching privacy than it would be to protect it.

This brief survey of the factors that influence private actors like ISPs and OSPs, consumers and governments indicate that it can be difficult to tailor a legislative scheme to promote citizens' notions of privacy. This analysis will inform my assessment of the voluntary disclosure scheme proposed in the *Protecting Canadians from Online Crime Act*.

C. VOLUNTARY DISCLOSURE PROVISIONS UNDERMINE THE PROTECTION OF PRIVACY

Voluntary disclosure provisions have the potential to undermine privacy protected by federal and provincial privacy legislation and undermine the constitutional protection against unreasonable search and seizure. They do so by creating incentives for ISPs, OSPs, and other firms to betray the privacy interests of their clients. While creating such incentives is not necessarily a violation of section 8 of the *Charter* as currently interpreted by Canadian courts, I suggest that perhaps it should be, because voluntary disclosure provisions may induce firms to disclose information to police that the latter would otherwise need a warrant to obtain. For instance, the *Protecting Canadians from Online Privacy Act* shifts onto service providers the responsibility to assess if the police request for subscriber information meets constitutional requirements; this is a function that our section 8 jurisprudence assigns to judges and officials with judge-like neutrality.[58] It ought not to be allocated to private corporations, especially given the incentives to act against their clients' interests discussed in the previous section.

The recent amendments to the *Criminal Code* contained in the *Protecting Canadians from Online Crime Act* make it very difficult for companies to assess whether to voluntarily disclose subscriber information. For instance, the new section 487.0195 permits them to disclose information that they are "not prohibited by law from disclosing."[59] The decision of a service provider to disclose information will be determined by its assessment of whether privacy protection legislation prohibits it from doing so. To take the example of *PIPEDA*, this assessment requires the ISP or OSP to know whether the police have "lawful authority to obtain the information" and whether they are using it to enforce "any law of Canada." If the police do not present a warrant when requesting the information, the question arises as to whether the police need one, which in turn requires the company to assess if the subscriber has a reasonable expectation of privacy in the information requested and whether the police are authorized to request it under a reasonable law. In his presentation to the Standing Senate

---

57 This is the implication of the Coase Theorem as applied to the analysis of law. See e.g. Acquisti, "The Economics of Personal Data," *supra* note 44 at para 13, citing Eli M Noam, "Privacy and Self-Regulation: Markets for Electronic Privacy" in US Department of Commerce, *Privacy and Self-Regulation in the Information Age* (Washington, DC: National Communications and Information Administration, 1997), online: Columbia University <www.citi.columbia.edu/elinoam/articles/priv_self.htm>.

58 *Hunter*, *supra* note 4 at 162.

59 *Criminal Code*, *supra* note 6, s 487.0195.

Committee on Legal and Constitutional Affairs, the Privacy Commissioner, Daniel Therrien, explained that this is "complex, highly contextual and difficult for organizations and individuals to undertake in each individual case."[60]

Not only is it difficult for a conscientious service provider to determine if the police have lawful authority to request the information without a warrant, the principal-agent problem identified in the previous section indicates that there are strong incentives for firms to under- or overprotect privacy. For instance, the firm may take into account its private interests when assessing whether to disclose even though these factors are not part of the legal analysis it should be conducting. Where voluntary disclosure provisions place responsibility to apply *Charter* tests such as that for assessing a person's reasonable expectation of privacy in the hands of private parties with incentives to misapply it, this arguably runs afoul of the requirement in *Hunter* that the balance of interests under section 8 should be determined *before* the search is conducted[61] (here, it is not determined at all by the state agents making the request) and by a neutral party capable of acting judicially.[62] It is of little consolation for a person whose privacy has been breached for a court to assert after the search has been conducted that the disclosure of subscriber information ought not to have occurred; by then, the investigation may have proceeded, charges been laid, and a prosecution commenced.

As we have seen, the interests of private companies are complex, and they do not necessarily line up with those of customers. Moreover, a legislative scheme may not constrain ISP or OSP behaviour if it does not create the right incentives for them, and so it may be unsuccessful in controlling firm behaviour. As a result, it is quite likely that OSPs or ISPs will choose to voluntarily disclose subscriber information to government agencies in situations in which a reasonable customer would expect them to protect their privacy. This is an example of a typical principal-agent problem — a problem in which the agent, in this case, the firm, may not do the bidding of the principal, in this case, the consumer. When legislation fails to strike a constitutionally required balance between competing interests — in this case, the public interest in law enforcement and the individual's privacy interests — it is arguably unlawful.[63]

ISPs and OSPs are not just bad agents for their clients — they are also bad agents for government. This occurs if service providers provide too much protection for their clients' privacy and fail to disclose information to police that would help a legitimate criminal investigation. In enacting the *Protecting Canadians from Online Crime Act*, the government may hope that firms will want to prevent their services from being used to acquire, trade, or store child pornography.[64] But this may not be the case, since the interests of government

---

60 Senate, Standing Committee on Legal and Constitutional Affairs, *Submission of the Office of the Privacy Commissioner of Canada on Bill C-13* (19 November 2014) (Chair: Hon Bob Runciman).

61 *Hunter*, *supra* note 4 at 160.

62 *Ibid* at 162.

63 The ineffectiveness of legislation was considered under the section 1 analysis in *Dagenais v Canadian Broadcasting Corp*, [1994] 3 SCR 835 at 886–87. Chief Justice Lamer noted that where the beneficial effects of legislation are limited, the consequent infringement of constitutionally protected rights outweighs the government's goal in pursuing the legislation, however meritorious it may be. See also the dissenting reasons of Justice Abella (McLachlin CJC, Binnie and LeBel JJ concurring) in *R v Bryan*, 2007 SCC 12, [2007] 1 SCR 527 at paras 124–25.

64 For instance, in *Ward*, Justice Doherty thought that firms, acting as good corporate citizens, are likely to want to prevent illegal use of the services they provide: *supra* note 13 at paras 102–103.

agents and private firms do not align. I have already mentioned one classic example above: a firm might decide to refuse all government requests for subscriber information if it thinks that such a decision is likely to retain or attract more customers, thus increasing its profitability.[65] Of course, weighing into this decision will be an assessment of what enforcement mechanisms the government has at its disposal, the risk that they will be deployed, and the cost to the firm of being found to have not complied with its legal obligations to disclose the information.

In the absence of incentives to make decisions that maximize public welfare, ISPs and OSPs are not good agents for either government officials or subscribers. Thus, voluntary disclosure provisions are unlikely to achieve a balance between the protection of privacy and the promotion of countervailing interests such as security that is defensible on constitutional grounds. If a firm were to adhere to *Charter* requirements, it would not disclose information that falls within a subscriber's reasonable expectation of privacy without being presented with a warrant. As I have noted, a firm is likely to over or underdisclose (that is, not adhere to privacy legislation or constitutional standards) depending on the costs and benefits of compliance or non-compliance.

D. EXISTING CASE LAW DOES NOT PROVIDE SUFFICIENT PROTECTION OF ONLINE PRIVACY

In the previous subsections, I demonstrated that voluntary disclosure provisions like those in the *Protecting Canadians from Online Crime Act* are not likely to result in appropriate levels of disclosure on the standards of either government or Internet users. The provisions inappropriately place the responsibility of deciding whether to provide private subscriber information to state agents on private companies, and these companies have incentives to disclose more than is in their clients' interest, but also less than governments might desire. Placing the responsibility in the hands of private companies is also problematic because section 8 of the *Charter* requires that searches by government agents be authorized prior to being conducted by a person capable of acting neutrally and impartially — a company's privacy compliance department is no substitute for judicial supervision of police searches.

It is now time to examine head-on whether voluntary disclosure provisions are unconstitutional. Some have speculated that such provisions in the *Protecting Canadians from Online Crime Act* would not meet constitutional standards after *Spencer*.[66] For instance,

---

[65] In the wake of the *Spencer* decision, both Rogers and Telus issued statements affirming that they would not disclose customer information to police without being presented with a warrant. Rogers asserts that it will only provide information if it gets "a court order or warrant" (Rogers, "How Rogers handles government requests for customer information" (5 June 2014) *Redboard*, online: <redboard.rogers.com/2014/06/05/transparency_report/>). See also Jim Bronskill, "Rogers, Telus won't give customer info to police without a warrant" *Toronto Star* (16 July 2014), online: <www.thestar.com/news/canada/2014/07/16/rogers_says_it_wont_hand_customer_info_to_police_without_a_warrant.html>.

[66] See Michael Geist's interpretation of *Spencer*: Michael Geist, "The Supreme Court Eviscerates Voluntary Disclosure, Part 1: Comparing Spencer with Govt's Claims," *Michael Geist* (blog), online: <www.michaelgeist.ca/2014/06/spencer-implication-part-1/>. See also House of Commons, Standing Committee on Justice and Human Rights, 41st Parl, 2nd Sess, No 30 (10 June 2014) at 2 (Daniel Therrien, Privacy Commissioner of Canada) [emphasis added]:

> Bill C-13 contains an amendment specifying that a person or organization enjoys legal immunity should they *voluntarily* preserve data or provide a document at an investigator's request without court authorization. We are concerned that this broad language could lead to a rise in additional

Michael Geist argues that, because *Spencer* concludes that a person has a reasonable expectation of privacy in subscriber information and this expectation is not diminished by exceptions in *PIPEDA* allowing voluntary disclosure, it should not be possible for the state to obtain it without a warrant.[67] A voluntary disclosure provision that permits or creates incentives for disclosure of information in these circumstances would thus facilitate an unreasonable search in the meaning of section 8 of the *Charter*. In this section, I argue that *Spencer* may not go that far. The Supreme Court of Canada leaves open the possibility that differently worded voluntary disclosure provisions and the contractual relations between the ISP or OSP and the subscriber may diminish a reasonable expectation of privacy. In such cases, a voluntary disclosure provision does not run afoul of the *Charter*. Of course, as we saw in the previous sections, I believe that legislation ought not to create incentives for service providers to violate constitutionally protected privacy interests.

My discussion of the constitutionality of voluntary disclosure provisions will address three important issues:

1. Do voluntary disclosure provisions authorize warrantless searches? [Section I.D.1.]

2. Do voluntary disclosure provisions limit a person's reasonable expectation of privacy, thus defining the scope of their section 8 *Charter* rights? [Section I.D.2.]

3. Do voluntary disclosure provisions undermine quasi-constitutional privacy protections[68] — that is, protections of privacy outside of the scope of section 8? [Section I.D.3.]

With respect to the first issue, the Supreme Court in *Spencer* affirmed that *PIPEDA* does not create new search or seizure powers. In regard to the second, the Court also concluded that the voluntary disclosure provisions in *PIPEDA* do not limit the scope of an individual's reasonable expectation of privacy. However, *Spencer* must be read narrowly: while voluntary disclosure provisions in a privacy-protection statute like *PIPEDA* and its provincial analogues do not compel ISPs or OSPs to disclose personal information in which an individual has a reasonable expectation of privacy, this does not preclude voluntary disclosure provisions in other statutes from doing so. In this light, section 487.0195 of the *Criminal Code,* an amendment introduced under the *Protecting Canadians from Online*

> voluntary disclosures and informal requests. This is of particular concern with private sector companies that are otherwise prohibited from disclosing personal information without consent under PIPEDA or substantially similar legislation. In essence, this could amount to permissive access without court approval and oversight.
>
> Ultimately then, we believe Canadians expect that their service providers will keep their information confidential, and that personal information will not be shared with government authorities without their express consent, clear lawful authority or a warrant.

67 See Geist, *ibid*.

68 Privacy statutes are considered "quasi-constitutional" because they protect interests that are necessary to the preservation of a free and democratic society: *Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401*, 2013 SCC 62, [2013] 3 SCR 733 at para 22 [*UFCW*]; *Lavigne v Canada (Office of the Commissioner of Official Languages)*, 2002 SCC 53, [2002] 2 SCR 773 at paras 24–25; *Dagg v Canada (Minister of Finance)*, [1997] 2 SCR 403 at paras 65–66; *R v Osolin*, [1993] 4 SCR 595 at 614; *Canada (Privacy Commissioner) v Canada (Labour Relations Board)*, [1996] 3 FC 609.

Crime Act, far from being unconstitutional, may play a role in narrowing constitutional protection.

With respect to the third issue, the Court confirmed in *Spencer* that, in certain circumstances, individuals can have a reasonable expectation that their use of the Internet will be anonymous. Anonymity is thus a new interest protected by section 8, consistent with the growing recognition of Canadian courts that new technologies like computers[69] and smartphones[70] create and facilitate new forms of social interaction that the public values. However, an expectation of online anonymity may not be reasonable in the face of a clear contract, privacy policy, or user agreement. In this situation, voluntary disclosure provisions may facilitate state access to private information by creating incentives for firms to disclose it even where statutory privacy protections are in place.

1. *SPENCER* DOES NOT REQUIRE THAT POLICE HAVE A WARRANT TO REQUEST INFORMATION IN WHICH A SUBSCRIBER HAS NO REASONABLE EXPECTATION OF PRIVACY

Prior to *Spencer*, the Crown had argued that the voluntary disclosure provision in section 7(3)(c.1)(ii) of *PIPEDA*, combined with section 487.014 of the *Criminal Code* (the predecessor of section 487.0195 introduced by the *Protecting Canadians from Online Crime Act*) authorized the police to request subscriber information; it did not matter, it argued, whether the police had a warrant to do so. The Crown's position would give great scope to a voluntary disclosure provision because it would in effect mean that an ISP or OSP could choose to voluntarily disclose information under *PIPEDA* in any situation in which police request it, thus overcoming the constitutional presumption that government agencies require a warrant to conduct such a search.

Some previous cases had accepted the government's argument that the "lawful authority" requirement in section 7(3)(c.i)(ii) of *PIPEDA* would be met if the police requested the information even though they did not have a warrant. However, in *Spencer*, Justice Cromwell is clear that police only have "lawful authority" to request information in the meaning of section 7(3)(c.1)(ii) if they have the power to *compel* disclosure, not just request it.[71] This power of compulsion exists, Justice Cromwell says, when police have a warrant, when they are using common law authority, or when they are conducting a warrantless search in exigent circumstances as authorized by common law.[72] In *Spencer*, the police were not authorized to request the information under any of these powers, and so the exception in *PIPEDA* was not engaged and disclosure was not permitted by it: the police had no warrant, so they were not authorized by statute to request the information; because the Court held that Spencer had a reasonable expectation of privacy in his subscriber information, the police could not use the common law power; and because there were no exigent circumstances they could not invoke the common law power to search and seize without a warrant.

---

69 *R v Vu*, 2013 SCC 60, [2013] 3 SCR 657 [*Vu*].
70 *Fearon*, *supra* note 16.
71 *Supra* note 13 at para 70.
72 *Ibid* at para 71.

While *Spencer* makes it clear that the voluntary disclosure provision in *PIPEDA* does not authorize an ISP or OSP to disclose subscriber information without being presented with a warrant, this does not mean that voluntary disclosure provisions *in general* do not diminish Internet privacy. Justice Cromwell also states in *Spencer* that where a person has no reasonable expectation of privacy in personal information protected by *PIPEDA*, the police have "lawful authority" in the meaning of section 7(3)(c.1)(ii) to obtain it under their common law power "to ask questions relating to matters that are not subject to a reasonable expectation of privacy."[73]

As we will see in the next section, a voluntary disclosure provision in a statute whose purpose is not the protection of privacy may eliminate an Internet user's reasonable expectation of privacy. Likewise, a clear contract, privacy policy, or user agreement between an ISP or OSP and their clients may eliminate the latter's reasonable expectation of privacy. In such a case, police have lawful authority to request subscriber information even though it is private personal information protected by privacy legislation and they do not require a warrant to do so. In such a case, the ISP or OSP can disclose the information to a law enforcement agency if they meet statutory requirements. Thus, voluntary disclosure provisions poke holes in the privacy protected both by the *Charter* and quasi-constitutional privacy statutes, and some, like section 487.0195(2), even create incentives for service providers to betray these privacy interests.

2. VOLUNTARY DISCLOSURE PROVISIONS MAY REDUCE THE SCOPE OF PRIVACY PROTECTION UNDER SECTION 8 OF THE *CHARTER*

In the previous section, I argued that *Spencer* confirms that a voluntary disclosure provision like section 7(3)(c.1)(ii) of *PIPEDA* and section 487.014 of the *Criminal Code* do not themselves authorize a police request for subscriber information without a warrant. But this does not mean that all such provisions have the same effect. In this subsection, I explain how *Spencer* is consistent with case law that allows voluntary disclosure provisions to narrow the scope of the protection against unreasonable search and seizure in section 8 of the *Charter*.

To explain how this occurs, it is necessary to have a clear understanding of the overlapping statutory and constitutional regimes. The statutory regime consists of federal and provincial privacy legislation, which provide "quasi-constitutional" protection of privacy. The other is section 8 of the *Charter,* which prevents unreasonable searches or seizures. To understand the interaction between the two, we will examine each in turn.

---

[73] *Ibid*. An example of this is *R v Devloo*, 2015 ABQB 345, 20 Alta LR (6th) 1 [*Devloo*]. The police were investigating Jared Devloo on suspicion of trafficking in cocaine. They had obtained information from WestJet that he would be flying from Winnipeg to Calgary on two separate occasions (*ibid* at paras 24, 44, 161, 163). The information was obtained without a warrant (*ibid* at para 45). With this information, they obtained a warrant to search Devloo's luggage after he had checked-in for his flight (*ibid* at para 47). Devloo argued that the police had obtained information from WestJet in which he had a reasonable expectation of privacy, thus violating section 7(3)(c.1) of *PIPEDA* and section 20(m) of *PIPA*. The judge held that Devloo had no reasonable expectation of privacy in the information (*ibid* at paras 200–205, relying on the authority of *R v Chehil*, 2009 NSCA 111, 248 CCC (3d) 370 [*Chehil*]). In consequence, he concluded that WestJet was authorized to disclose the ticketing information to police under *PIPEDA* (*Devloo*, *ibid* at paras 204–207).

Let's use *PIPEDA* as an example of typical privacy legislation.[74] Under the *Act*, an ISP or OSP may only collect, use or disclose "personal information"[75] with a person's consent and for purposes "that a reasonable person would consider are appropriate in the circumstances."[76] This provides quite a broad protection for personal information. However, it is slightly narrowed by an exception in the *Act*, which allows an ISP or OSP to disclose any subscriber information to a government agent if the agent requesting it has "lawful authority to obtain the information"[77] and the information is requested "for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law."[78]

A different kind of protection is provided by the *Charter*. Section 8 protects a person against unreasonable search or seizure of private information. Privacy is a value underlying this protection,[79] but there is not a free standing right to privacy under the *Charter*. "Private information" is defined in case law as information in which a person has a "reasonable expectation of privacy."[80] To obtain such information, a government agency must generally obtain a search warrant or production order[81] unless there are exigent circumstances or the common law authorizes a warrantless search.[82]

PIPEDA and section 8 of the *Charter* do not protect the same information in the same way. For instance, a person may not have a reasonable expectation of privacy in every kind of information that is considered personal information under *PIPEDA* or its provincial equivalents. In *Spencer*, the police sought to obtain the name, address, and telephone number of a customer using a particular IP address provided by the ISP, Shaw Communications.[83] Such information is personal information under *PIPEDA*, but until *Spencer,* it was a live issue as to whether a subscriber has a reasonable expectation of privacy in such generic information. Another controversial issue is metadata — data about a subscriber's use of an ISP's or OSP's services.[84] Does a subscriber have a reasonable expectation of privacy in data about how they use an ISP's or OSP's services?

---

74 The provincial equivalent in Alberta is *PIPA*, *supra* note 27, which applies instead of *PIPEDA*, *supra* note 13, in certain cases by virtue of section 4(6) of *PIPA* and section 26(2) of *PIPEDA*: see *UFCW*, *supra* note 68 at para 13.

75 Defined in *PIPEDA*, *ibid*, s 2. See also the similar definition of "personal information" in *PIPA*, *ibid*, s 1(1)(k).

76 *PIPEDA*, *ibid*, s 5(3); see also *PIPA*, *ibid*, ss 11, 19.

77 *PIPEDA*, *ibid*, s 7(3)(c.1). *PIPA* creates an exception in a slightly different way. Section 20(b) allows disclosure of information if it is authorized or required by a provincial or federal statute. Section 20(f) allows for the disclosure of information to a "public body or a law enforcement agency in Canada" that is conducting an investigation to enforce a law. Section 20(m) also allows disclosure if it is "reasonable for the purposes of an investigation or a legal proceeding." For an interpretation of how these provisions function, see *R v La*, 2012 ABQB 192, 285 CCC (3d) 332 [*La*].

78 *PIPEDA*, *ibid*, s 7(3)(c.1)(ii).

79 *Hunter*, *supra* note 4 at 159.

80 *Ibid*.

81 *Ibid* at 160.

82 *Spencer*, *supra* note 13 at para 71.

83 *Ibid* at para 11.

84 In *Vu*, *supra* note 69 at para 42, the Court may have gone some way to resolving this. It recognized that data about a person's internet activities contained on a computer (e.g., in the "internet history") enables police to obtain the kind of intimate information about a person's life that he or she would reasonably expect to be private. An argument can be made that this ruling can extend to metadata in the hands of an ISP or OSP.

How does a voluntary disclosure provision play into this mix? The purpose of a voluntary disclosure provision is to permit ISPs or OSPs to disclose information to law enforcement agencies. It can also create incentives for ISPs or OSPs to disclose information, for instance by removing liability for doing so. The exception in *PIPEDA* described above is a sort of voluntary disclosure provision because it gives a firm the discretion to disclose personal information when this is requested by an agency enforcing a law that has lawful authority to request it. Section 487.0195 of the *Criminal Code*,[85] introduced by clause 20 of the *Protecting Canadians from Online Crime Act*, does something substantially similar — it asserts that a person in possession of private information can voluntarily disclose it, and section 487.0195(2) adds that such a disclosure will not attract liability.[86] For instance, section 487.0195(2) would grant immunity to an ISP or OSP from prosecution for the tort of invasion of privacy when disclosing private information.[87]

What is the effect of this kind of voluntary disclosure provision on the section 8 analysis? Section 487.0195 was introduced to meet police concerns that it could not consistently obtain subscriber information; thus one can presume that the government's hope was to use this exception to reduce the reasonable expectation of privacy that a person has in personal information protected by privacy legislation, thus obviating the need for a warrant to obtain it. Case law has confirmed that legislative provisions and regulations can reduce the sphere of privacy in this way. In *R. v. Gomboc*, the Supreme Court of Canada recognized that a legislative or regulatory scheme is a factor to take into account when assessing if a person has a reasonable expectation of privacy.[88] Thus, in enacting section 487.0195 of the *Criminal Code*, the government may have hoped to erode the protection of section 8 of the *Charter* by creating a general provision authorizing voluntary disclosure of information.

In *Gomboc*, the Court dealt with whether the police violated Gomboc's rights by obtaining information about the electricity use in his house from the electricity utility. Gomboc had been operating a marijuana grow-op, and at the request of police, the utility installed an ammeter on the line into his house to determine how much electricity he was using.[89] On the basis of the information police acquired, they obtained a warrant to search the premises, which led to charges for producing and trafficking in marijuana. Part of the Crown's argument in that case was that Gomboc had no reasonable expectation of privacy in his energy consumption because of the contract between himself and the utility and because of a regulation made pursuant to Alberta's *Electric Utilities Act* which authorized the collection

---

85 *Supra* note 6. Section 487.0195 is a modification of the previous section 487.014, which also allowed voluntary disclosure to police where the person providing information was not prohibited by law from doing so. The difference is that section 487.0195 broadens the exemption from liability for providing the data to include exemption from both criminal and civil liability.

86 One possible consequence of the immunity from liability is that section 487.0195 could create an incentive for disclosure of private personal information in the meaning of *PIPEDA* in which a person does not have a reasonable expectation of privacy under section 8. For instance, in *Chehil*, *supra* note 73 at paras 23–24, the Court held that a person does not have a reasonable expectation of privacy under the *Charter* in his name, flight number, method of payment, and baggage allotment in the possession of an airline even though this is "personal information" in the meaning of *PIPEDA*.

87 Recognized as a possibility in *Somwar v McDonald's Restaurants of Canada* (2006), 79 OR (3d) 172 (Sup Ct J); *Nitsopoulos v Wong* (2008), 298 DLR (4th) 265 (Ont Sup Ct J); *Jones v Tsige*, 2012 ONCA 32, 108 OR (3d) 241. On the role of section 487.0195 of the *Criminal Code* in preventing liability on this ground, see House of Commons, Standing Committee on Justice and Human Rights, 41st Parl, 2nd Sess, No 22 (6 May 2014) (David Fraser).

88 2010 SCC 55, [2010] 3 SCR 211 [*Gomboc*].

89 *Ibid* at para 1.

of electricity use data through an ammeter. The regulation provided that a utility can voluntarily disclose customer information as long as it "is not contrary to the express request of the customer."[90] The Crown strengthened its argument by pointing to section 487.014 of the *Criminal Code*, which permits a peace officer to request a person to voluntarily provide information as long as that person is not prohibited by law from disclosing it.[91]

In a concurring judgement, Justice Abella (joined by Justices Binnie and LeBel) held that the regulation was determinative of Gomboc's privacy interest. Absent a challenge to the constitutionality of the regulation, she held that the clear statutory language eliminated any objective expectation of privacy:

> Absent a direct *Charter* challenge, we must presume the *Regulation* to be constitutional. And absent any ambiguity, we must treat its clear meaning as binding. According to the *Regulation*, the relationship between the customer and the company is such that the company is legally authorized to collect and disclose customer information to the police unless the customer expressly requests its non-disclosure. Mr. Gomboc made no request to the utility company to protect the confidentiality of his customer information. He therefore did not revoke the legislative authority that allowed [the utility company] to hand over his information to the police.[92]

Writing for the majority, Justice Deschamps disagreed that the regulation was determinative. In her view, the totality of the circumstances had to be considered, and the regulation was only one of the relevant circumstances.[93] However, while she did not consider the regulation determinative, she confirms its relevance to determining if the accused has a reasonable expectation of privacy. Interestingly, Justice Deschamps specifically points to section 487.014, the predecessor to section 487.0195, as likewise diminishing Gomboc's reasonable expectation of privacy in his electricity consumption. She writes that the Alberta regulation permitting voluntary disclosure

> dovetails with s. 487.014 of the *Criminal Code*, which confirms that a peace officer may ask a person to voluntarily provide information that the person is not otherwise prohibited by law from disclosing. Their combined effect establishes that not only was there no statutory barrier to [the utility company's] voluntary cooperation with the police request, but express notice that such cooperation might occur existed.[94]

The majority of the Supreme Court of Canada thus confirms that voluntary disclosure provisions can put a subscriber on notice that information will be disclosed on request, and this can diminish the scope of protection under section 8.

Only Justice Fish and Chief Justice McLachlin, dissenting, were of the view that the Court ought not to assume that a reasonable person would be aware of the regulation. They wrote that "[t]he average consumer signing up for electricity cannot be expected to be aware of the

---

90 *Ibid* at para 31.

91 *Ibid* at paras 31, 42. Note the similarity between section 487.014 of the *Criminal Code* and the new section 487.0195, which also expands the immunity of a person disclosing information from liability beyond what section 25 of the *Criminal Code* provides.

92 *Ibid* at para 91.

93 *Ibid* at para 33. For an interpretation of the Supreme Court of Canada's holding in *Gomboc*, see *La*, *supra* note 77 at paras 42–43.

94 *Gomboc*, *ibid* at para 31. This passage is cited in *La*, *ibid* at para 43.

details of a complex regulatory scheme — the vast majority of which applies to the companies providing services, and not to the consumers themselves."[95]

Doubtless, section 487.0195 was introduced into the *Criminal Code* to ensure that laws authorizing disclosure of customer information, such as the Alberta *Regulation* examined in *Gomboc*, would be considered when assessing a person's reasonable expectation of privacy. However, in *Spencer*, the Court held that section 7(3)(c.1) of *PIPEDA*, a voluntary disclosure provision, did not diminish Spencer's reasonable expectation of privacy.[96] We must thus turn to an examination of this case in order to see how *Spencer* modifies *Gomboc*. Does the former overrule the latter? Or is *Spencer* simply an application of *Gomboc* to a particular set of circumstances?

Our examination first requires us to clarify the relationship between section 8 and the exception in *PIPEDA.* The key question from the point of view of a law enforcement agency is — does the agency need a warrant to obtain information under the *PIPEDA* exception? There had been two answers to this question prior to *Spencer*.

a. Crown's Argument

In *Spencer,* the Crown argued that the exception in section 7(3)(c.1) of *PIPEDA* that permits disclosure of protected information affects the threshold requirement for section 8 protection, namely, the existence of a reasonable expectation of privacy.[97] A person cannot reasonably expect that subscriber information will be private if *PIPEDA* clearly provides an exception from this protection for disclosing this information to police.

b. Privacy-Protective Argument

The defence argued that *PIPEDA* plays no role in reducing a person's reasonable expectation of privacy, and so it does not affect whether police need a warrant to obtain information under the *PIPEDA* exception. Some laws or regulations may reduce privacy, but the mere existence of an exception to the protection of personal information in *PIPEDA* is not the kind of provision that can do this. Why? Because the exception is only triggered if the law enforcement agency can demonstrate that it needs the information to enforce a valid law and that the agency has "lawful authority" to obtain it. What this means in the *Charter* era is that the law enforcement agency must have a warrant or must be exercising some other power that would compel the ISP or OSP to disclose the information.

A number of cases prior to *Spencer* held that section 7(3)(c.1) of *PIPEDA* had the effect of decreasing a person's reasonable expectation of privacy in subscriber information in accordance with the Crown's argument explained above.[98] An example is *Ward*, in which Justice Doherty wrote that the provisions in *PIPEDA* put a subscriber on notice that an ISP

---

95 *Gomboc*, *ibid* at para 139.
96 *Spencer*, *supra* note 13 at 71–73.
97 *Ibid* at para 69.
98 *Ward*, *supra* note 13 at paras 47, 50; *R v Brousseau*, 2010 ONSC 6753, 264 CCC (3d) 562 at para 42; *Trapp*, *supra* note 13 at para 129 (interpreting a similar provision in Saskatchewan's *Freedom of Information and Protection of Privacy Act,* SS 1990-91, c F-22.01, the correlate to Canada's *PIPEDA*).

has the discretion to disclose private information, and that the company is likely to exercise this discretion in favour of police because it is reasonable to assume that an ISP will behave as a good corporate citizen. A corporation behaving in this way has an interest in preventing criminals from misusing the services it provides.[99] In pursuit of this interest, it would disclose subscriber information to the police in a criminal investigation if the request is sufficiently specific and limited.[100] Where there is no reasonable expectation of privacy, the government agent is under no obligation to obtain a warrant for a search or seizure. Thus, Justice Doherty wrote in *Ward*, *PIPEDA* affirms that a warrantless request for subscriber information is allowed as long as the request is specific and circumscribed.[101]

In *Spencer*, Justice Cromwell, writing for the Supreme Court of Canada, came to the opposite conclusion. In his view, the exceptions in *PIPEDA* allowing voluntary disclosure were subject to the general presumption created by that legislation that subscriber information was private and that the police must have a search warrant to obtain it.[102] In consequence, the exceptions in *PIPEDA* that allow ISPs or OSPs to voluntarily disclose subscriber information upon police request only allow disclosure where firms are presented with a valid search warrant or production order. The Court thus affirmed the privacy protective view as I have outlined above.

The broader question, though, is whether *Spencer* attenuates the general view expressed by a majority of the Supreme Court in *Gomboc* that voluntary disclosure provisions can narrow a person's reasonable expectation of privacy in subscriber information. If the cases are to be read consistently, the inevitable conclusion is that *Gomboc* states the general rule — such provisions can narrow a person's reasonable expectation of privacy — but where the voluntary disclosure provision is in legislation designed to protect privacy, it will not do so.[103]

3. CONTRACTUAL PROVISIONS AND THE REASONABLE EXPECTATION OF PRIVACY

In the previous section, we saw that voluntary disclosure provisions are relevant to whether a person has a reasonable expectation of privacy in a place or thing searched. In this section, I pick up on this discussion. In Section II.D.1, I explained that while voluntary

---

99 *Ward*, *ibid* at para 97.

100 *Ibid* at paras 96–102.

101 *Ibid* at para 108–109.

102 *Spencer*, *supra* note 13 at paras 62, 71, 73.

103 An example of the application of this interpretation is *Orlandis-Habsburgo*, *supra* note 28 at paras 2, 16, 39–41. The accused was charged with production of and trafficking in marijuana. Police had requested his electricity consumption records from his utility, which had voluntarily complied. The accused complained that this was a violation of *PIPEDA* and the *Municipal Freedom of Information and Protection of Privacy Act*, RSO 1990, c M.56 [*MFIPPA*]. Alternatively, he argued that if these statutes authorized the voluntary disclosure, the legislation violated section 8 of the *Charter*. In rejecting this argument, Justice Arrell held that the accused's expectation of privacy in the information was not reasonable due to the utility's conditions of service and the Ontario Electricity Board's Distribution System Code, which put a consumer on notice that unauthorized energy use will be reported to police. *MFIPPA* and *PIPEDA,* the judge concluded, affirmed the utility's right to disclose this information, which was otherwise private and to be protected, as they provided limited exceptions permitting disclosure as part of a criminal investigation involving misuse of the utility's services. Unlike in *Spencer*, if regulations in statutes that are not aimed at protecting privacy diminish a person's reasonable expectation of privacy, voluntary disclosure provisions will justify disclosure if the statutory requirements for such disclosure are met.

disclosure provisions do not create new powers for police to access subscriber information without a warrant, they can still create incentives for service providers to voluntarily disclose this information in circumstances in which a person has no reasonable expectation of privacy. The Supreme Court of Canada's decision in *Spencer* affirms that Canadians' privacy interests extend to online anonymity, and that this in turn entails that they have a reasonable expectation of privacy in subscriber information that, if disclosed, could reveal to state agents much of a person's online activities. But it is important not to exaggerate the protection that *Spencer* affords to subscriber information nor diminish the role that voluntary disclosure provisions can still play in creating incentives for ISPs and OSPs to disclose this information in certain cases. For instance, the terms of a contract, privacy policy, or user agreement between a service provider and its clients can narrow or eliminate their reasonable expectation of privacy, in turn leaving room for voluntary disclosure provisions to undermine Internet anonymity.

Spencer is the latest pronouncement on the role of contractual provisions, privacy policies, and user agreements on the reasonable expectation of privacy analysis. On the facts in *Spencer,* the Court found that the contract between the ISP, Shaw, and Spencer did not diminish Spencer's reasonable expectation of privacy in his subscriber information when interpreted in light of other documents.[104] In the Court's view, the contract, including Shaw's "Acceptable Use Policy" and its "Privacy Policy," was confusing and imprecise, and so it could not lead a subscriber to reasonably believe that he or she had consented to the disclosure of private information to law enforcement officials.[105] However, this fact-driven conclusion does not mean that contracts will never reduce the expectation of privacy. True, in *Spencer*, Justice Cromwell echoed Justice Deschamps' disapproval of contracts of adhesion in *Gomboc*.[106] In that case, Justice Deschamps reminded courts to "procee[d] with caution" when determining if such a contract narrows a reasonable expectation of privacy.[107] However, *Spencer* did not overturn the SCC cases that held that contractual provisions and other policies regulating a subscriber's use of a service are relevant to determining if section 8 is engaged.

In *Gomboc*, the majority affirmed that the terms in a contract between a user and a service provider — in that case, an electrical utility — should be considered when assessing if there is a reasonable expectation of privacy in information held by that provider.[108] It is thus possible that very clear contractual terms or a clear and detailed privacy policy could sufficiently diminish a customer's reasonable expectation of privacy in information he or she provides to the service provider. In *R. v. Cole*,[109] the Supreme Court examined the role of a school's workplace privacy policy in assessing if the accused had a reasonable expectation of privacy in a computer provided by his employer — a high school — that was used for personal purposes. Cole had used the computer to access child pornography. The employer's

---

104 *Supra* note 13 at para 66.

105 *Ibid* at para 60. Justice Cromwell began by examining Shaw's "Acceptable Use Policy" and "Privacy Policy" at paras 57–59.

106 *Ibid* at para 54. A contract of adhesion is a contract in which one of the parties has little choice but to sign the contract. Many consumer contracts are of this nature — they are long forms that the consumer may not understand. Moreover, he or she may not have any real choice but to accept the terms if all firms in the market offer basically the same contractual terms.

107 *Gomboc*, *supra* note 88 at para 33.

108 *Ibid* at para 54, Deschamps J; and para 94, Abella J (concurring on this point).

109 2012 SCC 53, [2012] 3 SCR 34 [*Cole*].

Acceptable Use Policy did not forbid using the computer for private purposes, but it did warn users that their files would not be private.[110] The majority concluded that

> [t]he policies, practices, and customs of the workplace are relevant to [assessing if the applicant has a reasonable expectation of privacy in the computer]. These "operational realities" may diminish the expectation of privacy that reasonable employees might otherwise have in their personal information.[111]

In applying this analysis to the facts in *Cole*, the majority concluded that, while the Acceptable Use Policy was relevant, it did not so diminish the expectation of privacy that section 8 was not engaged. The consideration of the totality of the circumstances led the Court to conclude that "[o]n balance, [the circumstances] support the objective reasonableness of Mr. Cole's subjective expectation of privacy."[112] It is possible to interpret the holding in *Cole* as standing for the proposition that a workplace privacy policy can never so diminish a reasonable expectation of privacy as to remove *Charter* protection from highly personal information. However, this reading is strained. The Court concluded that such policies are relevant to assessing the totality of the circumstances, but if they could never eliminate a reasonable expectation of privacy, this would make such policies irrelevant to this determination. The more accurate — though unfortunate — conclusion to be drawn from *Gomboc* and *Cole* is that clearly worded contracts, subordinate legislation, and workplace privacy policies can make a subjective expectation of privacy objectively unreasonable.

In light of this, *Spencer* must be read narrowly: while it affirmed that *PIPEDA* did not diminish Spencer's reasonable expectation of privacy, that expectation could have been narrowed had Shaw (Spencer's ISP) had a clearer contract and privacy policy.[113] Thus *Spencer* does not go so far as to say that if a customer read, understood, and signed a properly worded contract or privacy policy, he or she could not be said to have consented to the company's voluntary disclosure of information if requested by police.

The upshot of this analysis is this: *Spencer* leaves room for a reasonable expectation of privacy to be limited by a clear contract and privacy policy. If a person relinquishes their privacy interest in certain subscriber information, then a voluntary disclosure provision like that in the *Protecting Canadians from Online Crime Act* would remove barriers to disclosure that would otherwise exist in privacy legislation or at common law, thus paving the way for an ISP or OSP to disclose otherwise personal and private information to government agents. This conclusion is subject to two qualifications. First, exceptions to privacy law are subject to their own limitations. Section 7(3)(c.1)(ii) of *PIPEDA* requires the authority requesting the subscriber information to demonstrate that it has lawful authority to obtain it and that it is using it for law enforcement purposes.[114] Likewise, the voluntary disclosure provision in

---

110 *Ibid* at para 17.
111 *Ibid* at para 52.
112 *Ibid* at para 57.
113 For an example of a narrow reading of *Spencer*, see *R v Telus Communications Co*, 2015 ONSC 3964, 2015 ONSC 3964 (CanLII). Justice Nordheimer writes, "TELUS' own contractual documentation with its customers makes it clear that TELUS does not view the name and address of its subscribers to be private information" (at para 32).
114 *PIPA* is not as specific as to limits on disclosure. While *PIPEDA* limits disclosure to situations in which the agency requesting it has lawful authority to obtain it, *PIPA* limits disclosure of personal information in a more general way: the information may only be disclosed "for purposes that are reasonable," *PIPA*, *supra* note 27, s 19(1).

the *Protecting Canadians from Online Crime Act* only allows an ISP or OSP to disclose information if it would not otherwise be prohibited by law from doing so.

In conclusion, voluntary disclosure provisions, far from being unconstitutional after *Spencer*, still have a role to play. If the government or the market for Internet services creates incentives for ISPs or OSPs to provide clear wording in their contracts and privacy policies, a subscriber may no longer have a reasonable expectation of privacy in her private information. In such a case, a law enforcement agency could lawfully request it under *PIPEDA*. If *PIPEDA* did not apply, disclosure would be authorized — indeed, "incentivized" — under a voluntary disclosure provision like that in the *Protecting Canadians from Online Crime Act*. In such a case, the only thing protecting the privacy of subscribers of an ISP or OSP would be the values these firms place on attracting and retaining customers who are afraid of privacy breaches. Today, customers seem to demand privacy. But fear-mongering about crime and the predation of children could affect the political landscape, and so erode incentives for ISPs or OSPs to resist complying with police demands for their subscribers' information.

E. WHY THE PROTECTION OF ONLINE ANONYMITY SHOULD MAKE VOLUNTARY DISCLOSURE PROVISIONS UNCONSTITUTIONAL

We have established that it is at least arguable that Canadian case law does not render a voluntary disclosure provision such as that in the *Protecting Canadians from Online Crime Act* either useless or unconstitutional. But should it? I will end Part II by discussing the great innovation in *Spencer* — its recognition of online anonymity as an aspect of privacy protected by the Constitution. While we have seen that *Spencer*, *Gomboc*, and *Cole* leave a role for voluntary disclosure provisions to play, this is inconsistent with the Supreme Court of Canada's broadening of privacy to include online anonymity.

First, the holding in *Spencer* in regard to this new dimension of privacy. Without much normative argumentation, Justice Cromwell agreed that section 8 should protect a person's anonymous use of the Internet. The actual content of what we say, do, or access online may be public in the sense that it is easily viewed by other Internet users, but Justice Cromwell agrees with civil liberties organizations and privacy experts, who argue that anonymity is "one of the basic states of privacy."[115] Of course, the Court hedges slightly by saying that determining whether anonymity is protected "depend[s] on the totality of the circumstances."[116] But one could not expect the Court to do otherwise.

In my view, the recognition of the constitutional protection of online anonymity indicates that voluntary disclosure provisions in legislation of the kind the government has proposed to date are inherently problematic because they are based on the presumption that online anonymity is corrosive of public safety. Police and the government have sought to include voluntary disclosure provisions in the *Criminal Code,* privacy legislation, and other laws and

---

115 *Spencer*, *supra* note 13 at para 43, citing Alan F Westin, *Privacy and Freedom* (New York: Atheneum, 1967) at 31–32; 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) 57:4 Crim LQ 486 at 501.

116 *Spencer*, *ibid* at para 48.

regulations in order to ensure that subscribers cannot rely on anonymity to commit crimes. If courts uphold the legality of voluntary disclosure provisions as they appear to be doing, this will ultimately conflict with the public interest in online anonymity recognized in *Spencer*.

In a liberal democracy, the government must be required to justify why in any individual case the balance between safety and privacy tips in favour of safety. Existing voluntary disclosure provisions do not require transparency about how these competing interests are weighed. This lack of transparency means that the public cannot examine, much less challenge, the reasonableness of their decisions. In my view, this lack of transparency is not compatible with the burden of justification that the *Charter* imposes on the state to justify infringements of rights.

Richard Epstein puts this point in a different way. Courts, both in Canada and in the US, consider the legal arrangements between individuals and firms as well as the formal arrangements (laws and regulations) as factors in determining if the individual has a reasonable expectation of privacy in the information disclosed. We suppose that if a person is aware that the law allows voluntary disclosure, or that a contract permits such disclosure, he or she cannot have a reasonable expectation of privacy in information disclosed in this way. As Epstein points out, such arguments are circular, in that they provide no justification for why the legislator should permit this kind of invasion of privacy.[117] They draw a line between the public and private, but do not justify why the line is drawn in this place. Without a principled, or at least clear, way of drawing this line, privacy is always in danger.

III. WIDENING THE SPHERE OF CONSTITUTIONAL PROTECTION: SHIFTING THE BALANCING OF COMPETING RIGHTS TO SECTION 1 OF THE *CHARTER*

In Part II, I analyzed some laws that the Canadian government has proposed and passed that provide its agents with greater access to information that might disclose illegal activity. I ended by suggesting that if we take privacy rights seriously, voluntary disclosure provisions like those in the *Protecting Canadians from Online Crime Act* are inherently problematic. However, I also noted that such provisions are not necessarily unconstitutional based on existing case law. One can conclude from this that our case law is not in line with a defensible constitutional notion of privacy. In Part III, I explain why our section 8 jurisprudence has let us down by tolerating such inherently problematic provisions. I do so by tracing the history of the "reasonable expectation of privacy" cases. I also explain briefly why I think our constitutional law requires a different approach to the protection of privacy, and I suggest how to implement this in future cases.

The main problem I identify is that courts do not have a coherent approach to defining privacy. Instead, they allow the sphere of privacy to shrink or grow depending on the importance of countervailing public interests such as security. This is the wrong approach: the balancing of competing interests should be shifted to its proper place in the constitutional

---

[117] Richard A Epstein, "Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations" (2009) 24:3 BTLJ 1199 at 1206–1207.

analysis, namely, section 1 of the *Charter*. In this way, the onus is placed on the government to provide clear evidence of the necessity and proportionality of measures that infringe privacy rights. Likewise, the onus is placed on courts, by conducting an *Oakes* test, to be more clear and transparent about the reasons they believe interests such as security justify limiting the protection of privacy.

A. DEFINING PRIVACY: THE VIRTUES OF A BROADER APPROACH

The predominant approach to privacy in the section 8 case law does not adequately protect this important right. As we saw in Part II, courts have held that if a potential user of online services is informed about the kind of information an ISP or OSP is likely to disclose to third parties if she subscribes to the service, she may not have a reasonable expectation that this information will remain private. Voluntary disclosure provisions, when paired with a clear contract and privacy policy, may eliminate a subscriber's expectation of privacy.

There is nothing inherently problematic in the idea of limiting privacy based on contextual factors, nor in the idea that the scope of the privacy interest should be the gateway to constitutional protection. Thus, in its seminal case interpreting section 8 of the *Charter*, Justice Dickson, adopting the American approach under the Fourth Amendment, explains that it is only *reasonable* expectations of privacy that will be protected, thereby recognizing that the public interest may require limiting the scope of privacy protected by the Constitution.

But while it makes sense to limit the protection of privacy in the face of other important public rights and interests, how a court goes about balancing these interests is crucial. If courts limit privacy by considering countervailing interests when determining the meaning and scope of a person's privacy interest in the information the police seeks to obtain, courts may be balancing these interests without sufficient evidence and without giving the clear reasons that would have been required of them when they conduct a section 1 analysis. Courts should instead recognize broad privacy interests based on societal practices and use the *Oakes* test to engage in a more rigorous analysis of competing rights and interests.

As we will see, the problematic feature of Canadian section 8 jurisprudence is that courts take the first approach,[118] which often results in a narrow definition of privacy. This *ex ante* narrowing of the privacy interest usually involves intuitive reasoning in which courts draw analogies between the present case and past ones. For instance, in *R. v. Simmons,* the Court held that a person crossing an international border has a lower expectation of privacy simply because it is in the public interest to control who and what crosses the border.[119] However, few reasons are given to justify why the state interest in policing a border should have this result. The Court refers to the US case of *United States v. Ramsey*, in which Justice Rehnquist, writing for the Court, merely points out that such restrictions are "pursuant to the

---

[118] For example, Lisa Austin identifies three "ambiguities" in the section 8 jurisprudence, one of which is a shift "between a descriptive and a normative approach to defining privacy," while the other is a conflation of "the threshold question of defining privacy with the subsequent question of balancing privacy with other important social goals" (Austin, "Information Sharing," *supra* note 17 at 506).

[119] [1988] 2 SCR 495 at 526–27 [*Simmons*].

long-standing right of the sovereign to protect itself" and that they "should, by now, require no extended demonstration."[120] Chief Justice Dickson himself refers only to the importance of border searches for enabling the state to protect the general welfare of the nation[121] — there is no extended discussion of whether border searches are necessary, or whether they are proportionate to competing interests. In essence, the argument is that because we have always limited the scope of privacy at the border in the pre-*Charter* era, it makes sense that the right to privacy should be given roughly similar boundaries under the *Charter*.

The problem with this narrow approach is that it is circular — it does not ask the initial question about how to assess whether the law limiting privacy is justifiable in the first place.[122] To put this another way, such an approach does not explain *why* an individual has less privacy at the border than elsewhere. It merely narrows the normative concept of privacy based on the fact of greater scrutiny at a border.

The alternative is to define the scope of constitutionally protected privacy broadly, but then weigh an individual's particular claim to privacy against the public interest. Where the public interest outweighs the individual's privacy interest (and the public interest in protecting his privacy) the state may be allowed to invade it. This is how Canadian courts analyze many *Charter* rights — they define their scope broadly, but then allow the government to justify infringing them under the section 1 test.[123]

Why have Canadian courts chosen to narrow the scope of privacy rights based on competing interests rather than using section 1? One reason may simply be the wording of section 8, which only protects a person against an "unreasonable" search and seizure. Courts seem to have assumed that an assessment of what is "reasonable" (or "unreasonable") necessarily requires taking into account countervailing interests. After all, that's what "reasonable people" do — they weigh pros and cons. However, another interpretation of "reasonable" is that it invites a consideration of context, and doing this does not require the weighing of competing interests. Instead, it calls for "practical reasoning," that is, reasoning that applies norms to concrete factual situations.[124] This interpretation of reasonableness involves assessing what reasonable people generally consider to be private in a particular context regardless of countervailing public interests. An unreasonable search would be one that infringes what our public norms consider to be private. In the case of Internet privacy, the question is thus whether Canadians expect their anonymity to be preserved when using the Internet — a normative question about privacy in a specific context.

---

120 *Ibid* at 514–16, citing *United States v Ramsey*, 431 US 606 at 616–17 (1977).

121 *Simmons*, *ibid* at 526–27.

122 Epstein, *supra* note 56.

123 An example is the interpretation and application of section 2(b) of the *Charter*: see generally *CBC*, *supra* note 22.

124 For a description of this kind of practical reasoning, see Onora O'Neill, *Towards Justice and Virtue: A constructive account of practical reasoning* (Cambridge: Cambridge University Press, 1996) at 49, which describes "[a]ction-oriented conceptions of practical reasoning" as "seek[ing] to vindicate action, policies and characters as reasoned not by showing that they are constitutive of or instrumental towards ends of any sort, but, more directly, by showing that they embody certain types or principles of action, described with varying degrees of specificity or abstraction." In this case, the contextual reasoning called for does not justify a concept of privacy instrumentally, but rather as a principle in accordance which we can regulate the behaviour of individuals, private firms like ISPs and OSPs, and government agents — i.e., a principle for acting directed at a particular group of actors implicated in Internet usage.

Conceptually, it makes little sense to *define* rights based on conflicting interests. The Canadian constitution, unlike the American one, has a mechanism for balancing conflicting values — section 1 and the *Oakes* test — and it is thus not necessary to pre-empt the balancing that finds its proper place in a section 1 analysis by limiting the scope of protection afforded by section 8. Indeed, from a social welfare point of view, it is dangerous to do so, as it leads to an overly restricted sphere of privacy that does not accord with common perceptions of the harm caused by its invasion.

In the following sections, I describe some of the section 8 cases, identifying a general trend toward the problematic narrow approach to defining the scope of privacy, punctuated with moments of resistance.

B. DANGEROUS PRECEDENTS: DEFINING PRIVACY IN RELATION TO COUNTERVAILING PUBLIC INTERESTS

We have seen why it is notionally a bad idea to narrow the scope of privacy without being transparent about the reasons we protect it and how we justify limiting it. In this section, I briefly survey the source of the problem in the jurisprudence.

Arguably, it originates with *Hunter*, the seminal section 8 case. In that case, Justice Dickson sets out the Court's approach to the protection against unreasonable search and seizure, but he explains that he will do so without clarifying the relationship between sections 8 and 1.[125] In consequence of not having thought through the relationship between these two sections, there is a problem with the section 8 analysis that he carries out: it uses elements from what will emerge two years later as the section 1 analysis in *Oakes*[126] to define the scope of the right to a reasonable expectation of privacy protected by section 8. In consequence, factors that justify the state in limiting the right to privacy in *Hunter* are conceptually incompatible with the general broad and purposive approach that the Court takes to defining the scope of a *Charter* right.

Explaining the approach the Court wishes to take to defining the scope of a right, Justice Dickson outlines what he means by a purposive interpretation: sections of the *Charter* should be interpreted broadly in order to best fulfil a Constitution's goal, which is to "guarantee and protect" the rights and freedoms that it contains.[127] Applying this approach to the section 8 right against "unreasonable search and seizure," Justice Dickson takes as his starting point the impact of a particular search or seizure on its subject. This is not the time, he says, to consider if the search or seizure is a rational means of "furthering some valid government objective."[128] In the case of section 8, its purpose in the overall scheme of the *Charter* is to protect a person's reasonable expectation of privacy.[129] So far so good — the purposive approach involves a broad and liberal interpretation of the right protected by section 8 and eschews consideration of competing interests.

---

125 *Supra* note 4 at 169–70.
126 *Oakes*, *supra* note 23.
127 *Hunter*, *supra* note 4 at 156.
128 *Ibid* at 157.
129 *Ibid* at 159.

The problem arises with Justice Dickson's next move. After stating that the definition of *Charter* rights should not be limited by what is necessary to achieve other legitimate government objectives, he explains that section 8 only protects a "reasonable" expectation of privacy because there may be times when "the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals, notably those of law enforcement."[130] As we will see, subsequent cases have understood this to mean that the scope of a "reasonable expectation of privacy" is to be defined with reference to countervailing government objectives such as fighting crime.

However, this need not have been the turn taken in the case law. Justice Dickson's next move in *Hunter* suggests that his mention of the conflict between privacy and the state's interest in law enforcement was not intended to limit the scope of privacy protected by the *Charter*. Rather, having identified competing rights, Justice Dickson asks "how [is] this assessment to be made[?] When is it to be made, by whom and on what basis?"[131] This clearly indicates that his comment about the need to limit section 8 rights and to balance competing interests is relevant to determining the appropriate system for pre-authorization of intrusive searches; he is not suggesting that competing interests be used to define the scope of privacy. The system he recommends — a system of prior judicial authorization (search warrants) — requires that the person issuing the warrant determine when "[t]he state's interest in detecting and preventing crime begins to prevail over the individual's interest in being left alone."[132] However, at the warrant stage, the person deciding whether to issue the warrant does not have to define the scope of privacy. Rather, he or she is engaged in a sort of section 1 analysis — he or she must issue a warrant *in a particular case* by balancing competing rights and interests.

In early section 8 cases subsequent to *Hunter*, the Supreme Court of Canada did not use competing interests to define the right to privacy. In *R. v. Dyment*,[133] Justice La Forest begins by asserting the broad approach to interpreting *Charter* rights:

> From the earliest stage of *Charter* interpretation, this Court has made it clear that the rights it guarantees *must be interpreted generously, and not in a narrow or legalistic fashion*.… The function of the *Charter*, in the words of the present Chief Justice, then Dickson J., in *Hunter v Southam Inc.* … "is to provide … for the *unremitting protection of individual rights and liberties*". It is a purposive document and must be so construed. That case dealt specifically with s. 8. It underlined that a major, though not necessarily the only, purpose of the constitutional protection against unreasonable search and seizure under s. 8 is the protection of the privacy of the individual.… And *that right, like other Charter rights, must be interpreted in a broad and liberal manner so as to secure the citizen's right to a reasonable expectation of privacy against governmental encroachments.*[134]

Justice La Forest asserts competing government interests in encroaching on privacy ought not to be relevant to a broad and purposive interpretation of rights.

---

130 *Ibid* at 159–60.
131 *Ibid* at 160.
132 *Ibid* at 167.
133 [1988] 2 SCR 417 [*Dyment*].
134 *Ibid* at 426 [emphasis added].

Dyment involved the admissibility of blood samples taken from the defendant during a medical procedure at a hearing for charges of drunk driving. The blood had been obtained by the doctor without Dyment's awareness or consent, and it was then turned over to a RCMP officer, who had neither requested the sample nor obtained a warrant for it. Justice La Forest defines the right to privacy in these circumstances broadly. He looks first at what information is gathered from the blood and the use to which our society allows this information to be put, concluding that "to use an individual's blood or other bodily substances confided to others *for medical purposes* for purposes other than these seriously violates the personal autonomy of the individual."[135] Justice La Forest thus premises his assessment of a search's reasonableness on an evaluation of whether blood and bodily substances given for medical purposes contain information that our society considers private. In doing so, he does not place in the balance the state's legitimate interest in detecting crime. This is evident from the factors he considers when assessing the scope of a reasonable expectation of privacy, which include (1) the object searched or seized (in this case, blood); (2) the purpose for which the bodily substance was obtained (in this case, medical treatment). The state's interest in preventing crime plays no part at this stage in determining the scope of Dyment's interest in privacy.[136] He goes on to say that given the serious nature of the invasion of privacy in this case, a warrant is needed except in exigent circumstances. He affirms that while "[t]he needs of law enforcement are important, even beneficent, but there is danger when this goal is pursued with too much zeal."[137] A salutary caution.

Likewise, in *R. v. Mills*,[138] the Court also took a broad approach to protecting privacy. In that case, the judges dealt with the disclosure regime in sexual assault cases. Setting up such a regime necessarily involves the competing interests of the defendant's right to make full answer and defence, principles of fundamental justice promoted by section 7, the competing privacy interest of the complainant in her therapeutic records, and the equality rights of women and consequent need to protect their privacy in order to encourage the reporting of sexual assaults. In defining the scope of the complainant's section 8 interest, Justices Iacobucci and McLachlin properly interpret *Hunter*, stating that countervailing state interests may limit the protection a person's privacy, but that this balancing must be undertaken by the person issuing a warrant.[139] They affirm that balancing should only occur once "the nature of the interests at stake in a particular context" have been determined.[140] Justices Iacobucci and McLachlin do not use the balancing of rights to limit the definition of any particular right — for example, the right to make full answer and defence or the right to reasonable privacy. Instead, the balancing only serves to identify the appropriate "boundary between privacy and full answer and defence."[141] In other words, balancing delineates the boundary *between competing interests;* it does not serve to define what those rights or interests consist of.

---

135 *Ibid* at 436 [emphasis added].

136 Justice La Forest goes on to consider if there were exigent circumstances, but only after determining the scope of the privacy interest based on the thing searched or seized and the context in which it — in this case, a blood sample — was given.

137 *Ibid* at 436.

138 [1999] 3 SCR 668 [*Mills*].

139 *Ibid* at para 86.

140 *Ibid*.

141 *Ibid* at paras 92, 94.

Cases since *Dyment* and *Mills* have conflated the process of defining the scope of a privacy interest with the balancing of competing interests, which, in a constitutional case, ought properly to take place at the stage of a section 1 analysis, or in the case of a search warrant application, at the stage at which the judicial authority decides whether to issue the privacy-infringing warrant.

More recent cases have deviated from this approach, conflating the balancing of competing state interests with an evaluation of the objective reasonableness of the individual's expectation of privacy.[142] For example, in *Tessling*, Justice Binnie determines if a person has a reasonable expectation of privacy in information by striking a balance between privacy and the public interest. He writes,

> social and economic life creates competing demands. The community wants privacy but it also insists on protection. Safety, security and the suppression of crime are legitimate countervailing concerns. Thus s. 8 of the *Charter* accepts the validity of *reasonable* searches and seizures. A balance must be struck.[143]

Justice Binnie explains that this approach means that "the right to be free from examination by the state is subject to constitutionally permissible limitations."[144] The legal mechanisms used to limit the right to privacy are (1) defining what constitutes a "search" in a narrow way; (2) distinguishing reasonable from unreasonable expectations of privacy.

In *Tessling*, some of the factors the court considers in determining the reasonableness of the accused's privacy interest in heat escaping from his house should only be relevant to balancing a privacy interest against the state's interest in detecting crime. For instance, Justice Binnie considers the intrusiveness of the police search or seizure technique when determining the scope of the privacy interest.[145] Whether the technology used to conduct a search is intrusive is relevant to whether its use is proportionate to the infringement of the defendant's privacy,[146] but it should not be relevant to determining the scope of Tessling's privacy interest in the heat patterns escaping from his home. Indeed, the intrusiveness of the search was a decisive factor, because in Justice Binnie's view, obtaining an image of the heat emanating from Tessling's house by means of FLIR technology did not disclose information that was more than mundane about what was going on in the house.[147] Whether the information obtained from a search is mundane is not relevant to whether Canadians consider the information to be private. In the Internet context, subscriber information is mundane, but the presumption of Internet anonymity nevertheless warrants its protection.

---

142 As set out in *R v Edwards*, [1996] 1 SCR 128, determining if the defendant had a reasonable expectation of privacy in the person, place, or thing searched depends on determining both whether he had a subjective expectation of privacy and whether this expectation was objectively reasonable.

143 *Supra* note 18 at para 17 [emphasis added].

144 *Ibid* at para 18.

145 *Ibid* at paras 50–55.

146 The balancing involved when considering intrusiveness is clear from *R v Plant*, [1993] 3 SCR 281 at 295 [*Plant*]. In *Plant*, the police used a computer terminal linked to an electrical utility's computer to check Plant's consumption of electricity. Justice Sopinka, in considering that the search was not intrusive, concludes on this point that "[i]n addition to the fact that the manner and place of the search are indicative of a minimally intrusive search, the seriousness of the offence militates in favour of the conclusion that the requirements of law enforcement outweigh the privacy interest claimed by the appellant" (*ibid* at 295).

147 *Tessling*, *supra* note 18 at paras 46, 50. Justice Binnie cites *R v Buhay*, 2003 SCC 30, [2003] 1 SCR 631 at para 36 for support, but that paragraph merely says that if police do not have the grounds necessary to obtain a warrant, they must resort to investigative methods other than a search.

Finally, at the end of his evaluation of Tessling's reasonable expectation of privacy, we see where the conceptual error has entered into the section 8 test. Justice Binnie considers whether Justice Sopinka was right in *Plant* to consider whether the "seriousness of the offence" should be considered when determining the scope of a person's privacy interest. Although he concludes that it should not play a role at that stage, he does think that it is relevant to the overall section 8 analysis, in particular, to the determination of whether the search police conducted was reasonable.[148] Justice Binnie affirms that the seriousness of the offence committed by the offender is relevant to the "'balance' sought to be achieved in s. 8 of the *Charter*."[149] As I have argued, balancing ought to be undertaken either at the stage of a section 1 analysis or, in the case of the issuing of a warrant, at the point of judicial authorization.

Another example of problematic reliance on balancing in defining the scope of a privacy interest is in Justice Deschamps's dissenting reasons in *R. v. A.M.*[150] There, she argued that a student did not have a reasonable expectation of privacy in the contents of his backpack because the school where the search was conducted "was a school with a known problem of drug use by students,"[151] and all students benefit from a drug-free environment.[152] Here, again, the Court considers the state interest in preventing the sale of drugs in defining the privacy interest at stake.

Provincial courts of appeal have consistently used countervailing state interests to diminish the scope of privacy interests at the definitional stage. *Ward* is a good example in this regard. In that case, which involved the use of the Internet to obtain and store child pornography, the Court framed the section 8 inquiry as "whether the appellant had a reasonable expectation that he could anonymously access the Internet on his computer without the state, with the co-operation of the appellant's ISP, being able to find out what he had accessed."[153] Later on, in affirming that Ward did not have a reasonable expectation of privacy in his subscriber information, Justice Doherty again points out that the ISP's interest in helping to prevent the social harm caused by child pornography should have led Ward to expect that the subscriber information would be turned over to police if the latter requested it.[154] Here, the scope of Ward's privacy interest is being limited by the state's interest in preventing child exploitation and the steps the state and private actors like an ISP could reasonably be expected to take to pursue this interest.[155] I suggest that this is a classic example of balancing that should occur in a section 1 analysis. If we do not do so, the state is not required to explain, in a transparent and public way, why public interests outweigh private ones.

148 *Tessling*, *ibid* at para 64.
149 *Ibid*, citing *Plant*, *supra* note 146 at 295.
150 2008 SCC 19, [2008] 1 SCR 569.
151 *Ibid* at para 131.
152 *Ibid* at para 134.
153 *Ward*, *supra* note 13 at para 88.
154 *Ibid* at para 98.
155 *Ibid* at paras 102–103.

C. THE NEFARIOUS INFLUENCE OF THE US FOURTH AMENDMENT JURISPRUDENCE ON THE INTERPRETATION OF SECTION 8 OF THE *CHARTER*

I suspect that part of the problem that has emerged in Canadian case law is that Justice Dickson's interpretation of section 8 was highly influenced by American Fourth Amendment jurisprudence. Indeed, *Hunter* has an extensive discussion of *Katz v. United States*.[156] In American Constitutional law, there is no separate proportionality analysis. Thus the determination of what constitutes an unconstitutional search or seizure necessarily involves an assessment of its reasonableness. However, there are good reasons to abandon the US model once-and-for-all and separate the proportionality analysis from the definition of the scope of privacy: appellate courts in the US have questioned the ongoing relevance of the current approach to the Fourth Amendment. In *American Civil Liberties Union v. Clapper*,[157] the Second Circuit pointed out how inadequate the current analytical framework was for regulating modern technologies.

The jurisprudence under the Fourth Amendment does not protect privacy in documents disclosed to third parties.[158] To use the example of telephone records, the US Supreme Court held in *Smith* that a telephone user cannot reasonably expect his telephone records to be private when the telephone company must have access to them for the purpose of billing him.[159] This made sense in the days when such disclosure was relatively limited and when it was under the control of the individual. However, the Second Circuit points out that today,

> the very notion of an individual's expectation of privacy … may seem quaint in a world in which technology makes it possible for individuals and businesses (to say nothing of the government) to observe acts of individuals once regarded as protected from public view. On the other hand, rules that permit the government to obtain records and other information that consumers have shared with businesses without a warrant seem much more threatening as the extent of such information grows.[160]

The US Supreme Court has tried to get around the limitations of the Fourth Amendment jurisprudence. For instance, in *United States v. Jones*, the Court dealt with whether it violated the Fourth Amendment to place a GPS tracking device on the accused's car. The majority held that this constituted a search under the Fourth Amendment because placing the tracking device on the car was technically a trespass on the vehicle.[161] This avoided the problem of deciding whether the third-party doctrine applied because the accused had exposed his movements to the public, or whether the reasonable expectation of privacy test applied. In her concurring opinion, Justice Sotomayor noted that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties" because it is "ill suited to the digital age, in which

---

156 389 US 347 (1967).
157 785 F (3d) 787 (2nd Cir 2015) [*Clapper*].
158 *Smith v Maryland*, 442 US 735 (1979) [*Smith*]; *California v Greenwood*, 486 US 35 (1988), *United States v Miller*, 425 US 435 (1976) at 443; *Couch v United States*, 409 US 322 (1973).
159 *Smith*, *ibid* at 743–44.
160 *Clapper*, *supra* note 157 at 822–23.
161 *United States v Jones*, 132 S Ct 945 (2012) at 949–53.

people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[162]

It is now time to shed the influence of the restrictive interpretative framework that Canadian courts have adopted from US jurisprudence. With section 1 available and a well-developed jurisprudence interpreting the application of the *Oakes* test, there is no need to maintain the archaic restriction of privacy interests within the section 8 test. Indeed, since Parliament is often better placed than courts to assess the impact of new technologies and conduct a balancing of competing interests in this area, it makes sense to place the onus on government to provide convincing evidence as to the rationality and reasonableness of legislation that curbs privacy interests that are important to self-identity and our liberal democracy.

D. *R. v. Spencer* and *R. v. Fearon*: Signs of a New Approach?

It is hard to determine whether the Supreme Court's most recent cases, *Spencer* and *Fearon*, depart from or simply continue the approach of past section 8 case law. In *Spencer*, Justice Cromwell clearly departs from the approach of Justice Doherty in *Ward*. He rejects the view that the nature of the activity in which the defendant was engaged on the Internet — trading and downloading child pornography — is a factor in assessing Spencer's reasonable expectation of privacy in his subscriber information. Instead, the Court affirms that defendant's subscriber information is private because the activities one carries out on the Internet often disclose "intimate or sensitive activities" that one usually expects to be anonymous.[163] He implicitly criticizes Justice Doherty in *Ward*, stating that if we live in a state that protects privacy and takes legislative steps to protect it, such as contained in *PIPEDA*, one cannot use countervailing policy considerations to diminish privacy.[164] Rather than diminishing the scope of a privacy interest based on the importance of fighting child pornography, Justice Cromwell defines privacy normatively, taking into account constitutional and statutory protections of the right.

Indeed, there is some attempt in Justice Cromwell's reasons to connect online anonymity to the values underlying our Constitution. He cites Justice Doherty's comments in *Ward*, who writes that anonymity "is essential to the individual's personal growth and the flourishing of an open and democratic society."[165] While this point is not developed further, evidently, the Court was aware of the need to avoid the circularity identified by Epstein and to provide an independent normative justification for protecting privacy on the Internet. Justice Cromwell also points to a few earlier cases that take a similar normative approach, particularly cases in which the Court recognizes a reasonable expectation of privacy in information stored in personal computers, which usually contain personal information[166] and information that can

---

162 *Ibid* at 957.

163 *Spencer, supra* note 13 at para 66.

164 *Ibid* at para 63.

165 *Ward*, *supra* note 13 at para 71. On the importance of privacy for personal growth, see Stewart, *supra* note 41. See also Lisa Austin, "Privacy and the Question of Technology" (2003) 22:2 Law & Phil 119 at 147.

166 *Vu*, *supra* note 69 at para 41. See also *R v Morelli*, 2010 SCC 8, [2010] 1 SCR 253 at paras 3, 105; *Cole*, *supra* note 109 at para 47.

"enable investigators to access intimate details about a user's interests, habits, and identity."[167]

In both *Fearon* and *Vu*, the Supreme Court has also defined privacy interests broadly without restricting them unduly based on countervailing state interests. In *Vu*, the Court confirmed that the way that computers are used in our society today means that "[i]t is difficult to imagine a more intrusive invasion of privacy than the search of a personal or home computer."[168] They "store immense amounts of information"[169] and are constantly recording our online activities, making it possible to build a very detailed picture of our surfing history.[170] Likewise, in *Fearon*, Justice Cromwell acknowledged that cell phones — especially smartphones — are functionally equivalent to computers, and so a search of them "may constitute very significant intrusions of privacy."[171] In dissent, Justice Karikatsanis went further, connecting the privacy in cell phones to essential values of personal freedom and dignity.[172] She also acknowledged that this privacy is important for developing our identities as individuals, and that it facilitates our involvement in social life.[173]

The approach in *Spencer* and *Fearon* is welcome if it reflects a deeper recognition by courts that the scope of a privacy right ought not to be defined in relation to competing state interests. This recognition is essential to respecting a court's proper function in a liberal democracy. Aharon Barak asserts this in his discussion of balancing: "The concept of balancing recognizes that fundamental principles may conflict with one another, and that the proper resolution of this conflict lies *not in the elimination of the inferior value but in determining the proper boundary between the conflicting values*."[174] Implicit in this description is the idea that "fundamental principles" like privacy should first be properly defined before they are balanced.

Why is this so important? Because the order of operations reflects the proper role of a court in a democracy. As Dieter Grimm explains, courts are primarily engaged in a normative enterprise,[175] which involves defining norms and setting their limits. But setting limits always involves policy considerations, an area in which courts are not experts.[176] To overcome this gap in their expertise, when evaluating the effectiveness and efficiency of a legislative scheme, courts depend on the litigants to present them with evidence of the law's effects. Canadian courts have implicitly recognized this division of expertise in the structure of judicial review they have created. As Sujit Choudhry explains, the Supreme Court's interpretative methodology recognizes "that rights are of presumptive importance, and limitations the exception that are only acceptable if governments meet a demanding test of

---

167 *Vu*, *ibid* at para 42.
168 *Ibid* at para 40.
169 *Ibid* at para 41.
170 *Ibid* at para 42.
171 *Fearon*, *supra* note 16 at para 54.
172 *Ibid* at para 112.
173 *Ibid* at paras 112–15.
174 Aharon Barak, *The Judge in a Democracy* (Princeton, NJ: Princeton University Press, 2006) at 165 [emphasis added].
175 Dieter Grimm, "Constituitonal Adjudication and Democracy" in Mads Andenas & Duncan Fairgrieve, eds, *Judicial Review in International Perspective* (The Hague: Kluwer Law International, 2000) 111 at 114, 117.
176 *Ibid* at 117.

justification."[177] The section 8 inquiry does not have a mechanism for parties to present the kind of "clear, convincing and cogent" evidence that the Court has required before evaluating legislation that balances competing rights.[178] It thus lacks a key constitutional requirement of judicial review.

As we have seen, when Canadian courts evaluate search and seizure powers that limit privacy interests, they have not used a mechanism that reflects the division of powers and basic principles of constitutional review. They balance competing interests, but by not using the section 1 framework, they conduct the balancing in a somewhat intuitive way without proper consideration of the evidence they require. In consequence, their decisions on the proper balance between privacy and other rights and interests lack transparency — it is difficult for litigants to know how "privacy" will be defined in a particular case, since no clear definition is to be found in case law. Moreover, it is difficult to know what cases warrant limiting privacy interests, since courts do not review the necessity or proportionality of government limits on them.

IV. CONCLUSION

Privacy may be "a protean concept," as Justice Binnie opined in *Tessling*,[179] but our constitutional framework is designed to be a "living tree" that can accommodate shifting views about the reasonable scope of our private life. However, our courts have not adopted an approach to the protection of privacy under section 8 of the *Charter* that allows sufficient transparency about when and why privacy rights must yield to countervailing interests. Canadians clearly value online anonymity, a newly recognized form of privacy interest protected under the *Charter* since the Supreme Court's decision in *Spencer*. But courts place limits on this important interest *in the process of defining its scope* without rigorously inquiring into the proportionality of government measures to limit it. Without requiring the government to rigorously justify these limits in accordance with the *Oakes* test, courts have had to fall back on a largely intuitive approach to defining the scope of online privacy that is neither principled nor evidence-based.

In my view, the courts' approach to section 8 should be brought in line with the approach to other constitutional rights. Specifically, I have argued that the privacy interests underlying section 8 should be defined broadly based on the context in which a particular privacy interest arises, while the balancing of competing rights should be shifted to an analysis under section 1 of the *Charter*. This division between defining the scope of section 8 and assessing the proportionality of limits on the protection it provides would ensure that the government presents courts with evidence to justify laws that limit privacy. It would also ensure that courts are clearer about *why* they are placing certain boundaries on important and evolving privacy interests.

It follows from my suggestion about the proper approach to privacy under the *Charter* that certain kinds of legislative search and seizure schemes will necessarily be problematic. In

---

177 Choudhry, *supra* note 24 at 501–502.

178 The "clear, convincing and cogent" standard for a section 1 analysis was affirmed by Justice Rothstein in *FH v McDougall*, 2008 SCC 53, [2008] 3 SCR 41 at paras 39, 46.

179 *Supra* note 18 at para 25.

particular, a voluntary disclosure provision like that in the *Protecting Canadians from Online Crime Act* shifts the responsibility for balancing the privacy interests of subscribers against the public interest in disclosure, to private actors like ISPs and OSPs. Not only are the decisions of service providers not transparent, but their orientation toward profit has the potential to skew their decisions about disclosure away from an appropriate balance between crime prevention and privacy protection.

Despite being constitutionally suspect, under the current approach to section 8, voluntary disclosure provisions are likely constitutional. The Supreme Court of Canada has recognized that they have a role in determining the scope of a person's reasonable expectation of privacy. And where a person has no reasonable expectation of privacy, voluntary disclosure provisions lawfully create holes in the statutory protection of privacy. In my view, this is the unfortunate result of allowing privacy to be defined by the capacity of the state to invade it. Courts ought to require the government to explain why such invasions are necessary before finding the laws that facilitate them to be constitutional. Perhaps in future, courts will recognize the unacceptable circularity in the present approach to interpreting section 8 of the *Charter*.

Without holding the government accountable for intrusions into private life, governments may engage in unjustified fishing expeditions, accessing subscriber information without the protections that a warrant requirement provides, and undermining the protection of privacy through quasi-constitutional privacy legislation such as *PIPEDA* and its provincial equivalents. As the extent of state surveillance becomes more widely known, the threat that such fishing expeditions pose is ever more real.