Privacy and Civic Duty in *R v Ward*: The Right to Online Anonymity and the *Charter*-Compliant Scope of Voluntary Cooperation with Police Requests

*Andrea Slane**

R v Ward *was the third recent Canadian appellate court decision on warrantless police access to internet customer names and addresses. All three cases involved unsuccessful claims under section 8 of the* Charter. *Ward's claim failed because the cooperation by his internet service provider (ISP) with police was held to be reasonable, defeating the reasonableness of his expectation of privacy.*

In an era marked by increasing pressure on private actors to participate in law enforcement, the stakes are high for the future of online privacy protection under the Charter. *The author argues that the Ontario Court of Appeal's approach in* Ward, *while promising, must be further developed in order to protect the democratic values at the heart of section 8.* Ward *deserves credit for allowing private actors to consider both their customers' privacy and their own interests in assisting law enforcement. The Court of Appeal's analysis of the triangular relationship between police, defendant and ISP set principled limits on a private actor's ability to negate a defendant's reasonable expectation of privacy by cooperating with the police.*

However, the analysis of the reasonableness of the ISP's actions was based on a specific legislative standard. It could not fully reflect section 8's normative values, because that standard is contingent on the legislation and is not universally applicable. To remedy this problem, the author proposes a free-standing reasonableness obligation for third parties. While Ward *appeared to endorse this concept, it did not go far enough. An explicit free-standing obligation would ensure that private actors' discretion in cooperating with police investigations will be evaluated on the privacy standards we expect in a democratic society.*

* Associate Professor, University of Ontario Institute of Technology. The Privacy Commissioner of Canada funded research for this article. The author thanks Courtney McCarrell, Rajen Akalu and Linn Clark for their assistance with research and editing, and Lisa Austin and Simon Stern for their comments on earlier drafts.

Introduction

The Ontario Court of Appeal decided *R v Ward* on October 2, 2012, making it the third Canadian appellate-level decision within a year to focus on warrantless police access to internet customer name and address (CNA) information in the hands of internet service providers (ISPs).[1] *Ward* and two earlier Saskatchewan Court of Appeal cases, *R v Trapp*[2] and *R v Spencer*,[3] all held that the appellants' rights under section 8 of the *Canadian Charter of Rights and Freedoms*, which protects against unreasonable search and seizure,[4] had not been violated. However, each court arrived at their decision differently.[5] Of the three cases, *Ward* offers what I argue

1. 2012 ONCA 660, 112 OR (3d) 321.
2. 2011 SKCA 143, [2012] 4 WWR 648.
3. 2011 SKCA 144, [2012] 4 WWR 425 (released on the same day as *Trapp*).
4. Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11 ("[e]veryone has the right to be secure against unreasonable search or seizure", s 8).
5. Justice Cameron wrote the majority judgment in *Trapp* (joined by Jackson JA), and Ottenbreit JA wrote concurring reasons. Justice Caldwell wrote alone in *Spencer*, with Cameron and Ottenbreit JJA writing separate concurring reasons aligned with their reasons in *Trapp*. Justice Doherty wrote for the Ontario Court of Appeal in *Ward* (joined by Winkler CJO and Goudge JA).

is the most promising approach to determining when a person's online anonymity can be legitimately unmasked through a third-party service provider's voluntary cooperation with police. However, *Ward* may still have failed to meet the normative approach to section 8 rights laid down by the Supreme Court of Canada in *R v Duarte*: whether "the standards of privacy that persons can expect to enjoy in a free and democratic society"[6] were duly respected in the circumstances.

The facts in *Ward* are similar to those of virtually all other Canadian cases dealing with warrantless police access to CNA information.[7] Police had evidence of someone downloading, accessing or sharing child pornography at a particular date and time and they identified the Internet Protocol (IP) address used to do this. Using public records, they determined which Canadian telecommunications company hosted the IP address and a general location of the user.[8] Police then sent a "letter of request" (a form letter developed by police in partnership with service providers[9]) asking the ISP to voluntarily disclose "the name and address of the subscriber associated with an IP address used on June 16, 2006 between 06:09:24 and 06:09:48, a span of 24 seconds. The other two requests relating to connections made on July 2 and July 6 referred only to a single point in time."[10] The ISP obliged. The police investigated the inhabitants of the

6. [1990] 1 SCR 30, 71 OR (2d) 575.

7. For other trial-level cases that were not appealed, see *R v Kwok* (2008), 78 WCB (2d) 21 (available on QL) (Ont Ct J); *R v Friers*, 2008 ONCJ 740 (available on QL); *R v SWF*, 2009 ONCJ 103 (available on CanLII); *R v Verge*, [2009] OJ no 6300 (QL) (available on WL Can) (Ct J); *R v Vasic* (2009), 185 CRR (2d) 286 (available on CanLII) (Sup Ct J); *R v Cuttell*, 2009 ONCJ 471, 247 CCC (3d) 424; *R v Wilson*, [2009] OJ no 1067 (QL) (available on WL Can) (Sup Ct J); *R v McNeice*, 2010 BCSC 1544 (available on CanLII); *R v Brosseau*, 2010 ONSC 6753, 264 CCC (3d) 562.

8. See *R v Ward*, *supra* note 1 at paras 27–32. A website operator featuring user forums, carookee.com, became aware that some users of its site were exchanging child pornography and provided IP addresses to German police (the site is based in Germany). German police sorted the IP addresses by geographic location, and notified the RCMP of those IP addresses located in Canada. The RCMP determined that three of the IP addresses were assigned to Bell Sympatico in the Sudbury, Ontario area. These were subsequently identified as having been used by the defendant's account at the relevant dates and times. *Ibid.*

9. See Suzanne Morin, "Updated: Business Disclosure of Personal Information to Law Enforcement Agencies: PIPEDA and the CNA Letter of Request Protocol", *Privacy Pages: CBA National and Privacy Access Law Section Newsletter* (November 2011), online: The Canadian Bar Association <http://www.cba.org>.

10. *R v Ward*, *supra* note 1 at para 25.

address and what type of internet connection they used[11] and obtained a warrant to search the computer equipment at the address. The search yielded further evidence of child pornography offences with which the accused was charged. He invoked section 8 of the *Charter* to challenge the constitutionality of how the police identified him with his initial internet activity. Like the defendants in most similar section 8 cases, David Ward's *Charter* challenge failed, for reasons I will explore below.

Courts have approached the problem of whether ISP disclosure of CNA information to police without a warrant complies with the *Charter* based on the Supreme Court of Canada's analysis of warrantless third-party information disclosure in other contexts, most commonly with reference to electrical utility customers.[12] As in all section 8 cases, the inquiry involves two parts: determining whether the defendant's subjective expectation of privacy in the information at issue was reasonable; and if so, determining whether the search itself was reasonable.[13]

The first stage of the inquiry focuses on the subject matter of the alleged search. If it is the kind of information that section 8 protects—i.e., for which a person can legitimately claim an expectation of privacy—then the first stage continues and focuses on whether that expectation is objectively reasonable in the circumstances. This inquiry into reasonableness must consider the totality of the circumstances, including any relevant factors

11. Residences with multiple inhabitants or a wireless internet connection pose greater difficulties for determining who was actually using the IP address at the relevant times. In most of the decided cases, the defendant lived alone (or, as in *Spencer*, with one other person) and used a wired internet connection.

12. See e.g. *R v Plant*, [1993] 3 SCR 281, 145 AR 104 [cited to SCR]. In *Plant*, Sopinka J set out the scope of section 8 protection of informational privacy, writing that it should seek to protect a "biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state", including information that would tend to "reveal intimate details of lifestyle and personal choices of the individual". *Ibid* at 293. The Supreme Court further refined the analytical framework for determining the reasonableness of an expectation of privacy where information is held by a third party. See *R v Gomboc*, 2010 SCC 55 at para 32, [2010] 3 SCR 211. Other cases have also recognized that a reasonable expectation of privacy adheres to certain locations and personal belongings (e.g., a purse or backpack) regardless of the sensitivity of the actual contents. See e.g. *R v AM*, 2008 SCC 19 at para 73, [2008] 1 SCR 569.

13. These two steps are set out in *R v Edwards*. [1996] 1 SCR 128 at para 33, 132 DLR (4th) 31.

such as the relationship between the third party and the defendant as set out by legislation or contract.[14] If the court finds that the defendant has a reasonable expectation of privacy in the information provided by the third party, it proceeds to the second stage of the inquiry: whether the warrantless search was reasonable. A warrantless search is presumptively unreasonable, but is deemed to be reasonable if it is authorized by law, if the law itself is reasonable and if the search is carried out in a reasonable manner.[15]

The CNA cases, including *Ward*, *Spencer* and *Trapp*, have made important contributions to the section 8 jurisprudence on online anonymity. The *Ward* judgment did not require a warrant for all police access to CNA information linked to internet activity, so it did not go as far as many privacy advocates had hoped.[16] However, it did pull back from a trend toward much wider access to CNA information by proposing some constraints on third-party warrantless cooperation with police. Specifically, *Ward* circumscribed the scope of warrantless access to CNA information by requiring ISPs to balance their own legitimate interest in policing their networks with their obligation to protect customer privacy. I do not disagree with the conclusion reached in *Ward*. In fact, in this comment I will explore how aspects of the *Ward* judgment have improved the approach of Ontario courts to third-party voluntary cooperation with police investigations. However, I will also suggest that further improvement is needed in the form of a free-standing reasonableness requirement that would apply to third-party decision

14. See *R v Plant*, *supra* note 12 at 292–93; *R v Gomboc*, *supra* note 12 at para 57.

15. See *R v Collins*, [1987] 1 SCR 265 at 278, 38 DLR (4th) 508.

16. See Stephen Neil, "Law Enforcement Wins at the Expense of Internet Privacy in *R v Ward*" (9 October 2012), online: The Court <http://www.thecourt.ca>; "Ontario Court of Appeal Rules on Warrantless Access to IP Addresses and Customer Names" (2 October 2012), online: Canadian Civil Liberties Association <http://ccla.org>; Jesse Brown, "Think You Have a Right to Privacy Online? Think Again, Says Ontario Court" (4 October 2012), online: Maclean's <http://www2.macleans.ca>; David Fraser, "Ontario Court of Appeal Rules no Expectation of Privacy in Connecting IP Address to Customer Name" (2 October 2012), online: Canadian Privacy Law Blog <http://blog.privacylawyer.ca>.

making in dealings with police, and that could be called upon in the first part of the section 8 analysis.[17]

Without a free-standing obligation to act reasonably, the legislative and contractual regimes that constrain and shape the private sector's response to police requests for customer information will not necessarily reflect the privacy standards we should expect in a democratic society.[18] Too much is left to social convention and political will. *Ward* did not resolve this difficulty. The decision was tied too closely to the specific governing legislation, in this case the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*).[19] That is, the normative standard for judging the reasonableness of the third party's actions was only located within that legislation, so the third party's reasonableness appropriately formed a part of the contextual section 8 inquiry. But if the reasonable expectation of privacy is to be a normative standard, third-party reasonableness in customer information disclosure must *always* factor into whether the defendant's expectation was reasonable, regardless of whether legislation compelled the third party to act reasonably.

I will begin with the praiseworthy aspects of *Ward*, explaining how it strengthened section 8's protection of online anonymity and constrained third-party voluntary participation in crime control and investigation. I will then situate *Ward* in its historical context by exploring how ISPs

17. Because the Court in *Ward* found that the appellant had no reasonable expectation of privacy in his account information in these circumstances, it did not have to determine whether the initial police request itself was reasonable or whether the law authorizing such requests was reasonable. In *Trapp*, the Court decided that the appellant did have a reasonable expectation of privacy in his subscriber information, so the decision turned on the second part of the section 8 analysis, which asked whether the search itself was reasonable. *Supra* note 2 at paras 66–71. While the question is beyond the scope of this comment, I would argue that if there are no constraints on the reasonableness of police requests other than legislation that may or may not require a third-party service provider to act reasonably, then the overarching regime authorizing police to ask for this information is not reasonable either. If police requests were instead judged by reference to the degree of voluntary cooperation by third parties that is normatively reasonable in a democratic society, we would stand a much better chance of preserving an appropriate balance between informational privacy interests and effective law enforcement.

18. In order to achieve a rigorous normative evaluation of the current regime, it may be necessary for a defendant to bring a *Charter* challenge directly to the specific provisions of the legislation that permit police to ask for customer information, and permit third parties to provide it in a given case. See *R v Gomboc*, *supra* note 12 at para 86.

19. SC 2000, c 5 [*PIPEDA*].

have responded to the development of an approach to crime control that strongly encourages the participation of civil society. This context will allow a more rigorous evaluation of the *Ward* Court's claim to have met the required normative standard of privacy protection. Lastly, I will argue that the courts must establish a free-standing obligation on third parties for reasonable disclosure of customer information, modelled on *Ward*'s interpretation of the privacy obligations of third parties under *PIPEDA*. The Supreme Court of Canada is expected to weigh in on these issues soon, having granted leave to appeal in the *Spencer* case, which has similar facts to *Ward*.[20]

I. Praiseworthy Aspects of *Ward*

A. Clarifying the Right to Online Anonymity

The first step in a section 8 analysis involves assessing whether the subject matter of the search—in this case, CNA information—is the kind of information a person can reasonably expect to shield from state intrusion.[21] Parties to CNA disclosure cases have characterized this subject matter in various ways. Crowns have argued that CNA information is not sensitive, is frequently shared, and consequently is not the kind of information that deserves section 8 protection.[22] In contrast, defendants have argued that access to CNA information should always require a warrant, as it can identify a person who has deliberately engaged in anonymous internet activity, potentially revealing deeply personal information about his or her online activities.[23]

(i) The Degree of Protection for CNA Information

Like *Spencer* and *Trapp*, *Ward* gave some weight to the argument that CNA disclosure can reveal sensitive personal information because

20. *R v Spencer*, *supra* note 3, leave to appeal to SCC granted, 34644 (January 24, 2013).
21. See *R v Edwards*, *supra* note 13.
22. See e.g. *R v Trapp*, *supra* note 2 at para 34; *R v Spencer*, *supra* note 3 at para 23; *R v Ward*, *supra* note 1 at para 10.
23. See e.g. *R v Trapp*, *supra* note 2 at paras 23–24; *R v Spencer*, *supra* note 3 at paras 11–12; *R v Ward*, *supra* note 1 at para 6.

it de-anonymizes internet activity that the defendant clearly intended to hide.[24] Both the Saskatchewan and Ontario appeal courts rejected the Crown's characterization of the information that the police were seeking as merely a name and address.[25] As the courts recognized, the police had no intrinsic interest in the CNA information itself, but sought to use it to identify the person who had engaged in particular internet activity. This distinguishes CNA information in the internet context from situations where the name of an account holder has generally not been protected, e.g., in cases where the police have asked banks to confirm the name associated with a bank account number written on fraudulently-cashed cheques.[26] In the banking example, disclosing the account holder's name reveals nothing further about that person's banking activity, but disclosure of CNA information by an ISP has what the *Ward* judgment said was the "very real potential to reveal activities of a personal and private nature".[27]

Two features of the decisions in *Ward*, *Trapp* and *Spencer* are important to the scope of protection for online anonymity. First, the courts differed in how they characterized the range of personal activities that could be revealed by the CNA information requested from ISPs. Second, the *Ward* decision alone helpfully situated the request at issue within the specifically *public* online context in which police initially became aware of the defendant's illegal activity.

In *Trapp*, the Saskatchewan Court of Appeal came the closest to accepting the defendant's position. Identifying a customer's IP address, the *Trapp* judgment said, can provide a "complete history of [the defendant's] activity on [the Gnutella] network. And apparently this is but the beginning of what someone might learn of another if supplied with the identity of the person to whom an IP address is assigned."[28] However, this holding might be specific to the file-sharing context at issue in *Trapp*.

24. *R v Trapp*, *supra* note 2 at paras 35–40; *R v Spencer*, *supra* note 3 at paras 22, 42, 98; *R v Ward*, *supra* note 1 at paras 89, 92.

25. But see *R v Trapp*, *supra* note 2 at para 134, Ottenbreit JA. Only Ottenbreit JA (writing separate concurring reasons in both *Trapp* and *Spencer*) accepted the Crown's position that customers have no reasonable expectation of privacy in CNA information by virtue of its non-sensitive nature. See also *R v Spencer*, *supra* note 3 at paras 109–10, Ottenbreit JA.

26. See *R v Quinn*, 2006 BCCA 255 at paras 90–93, 209 CCC (3d) 278.

27. *Supra* note 1 at para 93.

28. *Supra* note 2 at para 36.

In contrast, the courts in *Ward* and *Spencer* rejected the defendants' argument that unmasking an anonymous online identity associated with an IP address gave police broad access to the history of an account holder's internet activity.[29] Instead, the Court in *Ward* stressed that because IP addresses are only temporarily assigned to a particular subscriber, and may even change during the course of a particular session, the identifying information the police sought could only provide something "more in the nature of a snapshot than a history of one's Internet activity".[30] The Court acknowledged that its view would have been different if IP addresses were permanently assigned to particular subscribers or could otherwise reveal a longer history of internet use, as was the case in *Trapp*.[31]

(ii) The Public Nature of Internet Use and Privacy Expectations

The *Ward* Court held that the public nature of the defendant's anonymous activity reduced the degree of protection that the accused could reasonably expect, but did not eliminate all privacy claims. In *Ward*, the police came upon child pornography files being shared through a public web forum.[32] Ward's use of a temporary email address, however, clearly indicated his intention to protect his online activity from scrutiny. The Court dealt with this conflict by expressly characterizing the right to remain anonymous in these circumstances as an aspect of "public privacy"—i.e., where a person has a right to move about in public spaces without constant state surveillance, although with less of an expectation of privacy than in private spaces.[33]

Ward noted that section 8 case law acknowledges that the privacy it protects is "about more than secrecy and confidentiality", in that a person in a democratic society should not fear being "called to account for

29. *R v Ward*, *supra* note 1 at para 69, citing *R v Trapp*, *supra* note 2 at para 36; *R v Spencer*, *supra* note 3.

30. *Supra* note 1 at para 18.

31. *Ibid* at para 109.

32. *Supra* note 1 at paras 27–28. The website at issue allowed any user to establish a public forum using an email address, including an anonymous one, and it was the website operator who reported illegal content to police. In the other two cases, police combed file-sharing programs looking for publicly-accessible child pornography (via LimeWire in *R v Spencer*, and Gnutella in *R v Trapp*). *Supra* note 3 at paras 5–6; *supra* note 2 at para 77.

33. *R v Ward*, *supra* note 1 at paras 72–73.

anything and everything one does, says or thinks".[34] Section 8 is intended to allow individuals to live while "enjoying a degree of anonymity that is essential to the individual's personal growth and the flourishing of an open and democratic society".[35] However, where police have evidence of specific criminal activity, the public interest in effective law enforcement is heightened. In these cases, identifying the parties in the public space where the criminal activity occurred is justifiable in ways that monitoring general public activity is not.[36] The problem is to determine precisely what degree of anonymity in public online forums is protected from warrantless police access. The *Ward* Court focused on this issue in the next part of its section 8 analysis, exploring the reasonableness of a defendant's expectation of privacy in the particular circumstances.

II. Reasonable Expectations of Privacy in the Context of Third-Party Voluntary Cooperation with Police Investigations

After establishing that CNA information qualifies for protection under section 8, the *Ward* decision dealt mainly with whether the appellant had a reasonable expectation of privacy. The right to be secure against unreasonable search or seizure involves a balancing exercise. What has to be assessed is whether "in a particular situation the public's interest in being left alone by [the] 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".[37] When police seek information held by a third party, a triangular relationship is formed between the defendant, the third party and the police. The third party

34. *Ibid* at para 71.

35. *Ibid*.

36. The Information and Privacy Commissioner of Ontario has suggested, for instance, that an "incident driven" approach to police access to video footage from public transit vehicles and platforms is an appropriate limitation on the use of surveillance video. Information and Privacy Commissioner of Ontario, News Release, MC07-68, "Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report" (3 March 2008), online: IPC <http://www.ipc.on.ca> at 17.

37. *R v Ward*, *supra* note 1 at para 79, citing *Canada (Combines Investigation Branch, Director of Investigation and Research) v Southam Inc*, [1984] 2 SCR 145 at 159-60, 11 DLR (4th) 641 [*Southam*].

mediates a relationship which is directly governed by the *Charter*—that between the defendant and police.

As *Ward* noted, Canadian privacy jurisprudence has emphatically rejected the "risk analysis" approach common in American Fourth Amendment case law, so that "allowing others into a zone of personal privacy, does not forfeit a claim that the state is excluded from that same zone of privacy".[38] In other words, even when a defendant has allowed a business to access her personal information (in this context, by necessity in order to use the service), this does not mean that this information is automatically fair game for police, as would be the case in the United States.[39] However, the Supreme Court of Canada has also stated that when information lies in the hands of a third party, a person's expectation of privacy will generally be reduced, unless an obligation of confidentiality is established.[40] As *Ward* put it, "it is necessary to look at the controlling contractual and legislative provisions when determining whether a person has a reasonable expectation of privacy in information that a third-party service provider has given to the police".[41]

The relationship between the police and the third party is governed by intersecting legislative regimes that appear to permit police to ask for (and businesses to provide) information related to an investigation.[42] In turn, the relationship between the ISP and the defendant is governed by contract, which is relevant to the level of confidentiality the defendant can expect. In *Ward*, the Court's analysis of the standard of reasonableness required of private organizations under *PIPEDA* was quite detailed and robust, and influenced the Court's reading of the contract. *Ward* therefore contributes to the jurisprudence dealing with the reasonableness of a business' decision to voluntarily disclose information to police. But *Ward* did not go far enough—rather, it limited the analyses to *PIPEDA*. *Ward* did, however, endorse the possibility of free-standing obligations for businesses to act reasonably when responding to police requests, as set

38. *Supra* note 1 at paras 76–77, citing *R v Duarte*, *supra* note 6; *R v Wong*, [1990] 3 SCR 36, 1 CR (4th) 1 [cited to SCR].

39. See *United States v Miller*, 425 US 435 at 442–43 (1976).

40. *R v Plant*, *supra* note 12 at 294; *R v Gomboc*, *supra* note 12 at paras 30–33.

41. *Supra* note 1 at para 95.

42. See *ibid* ("[t]o properly describe the relationship between the appellant and [the ISP], one must first properly characterize [the ISP]'s relationship with the police insofar as the request for the appellant's subscriber information is concerned" at para 96).

out briefly in *Trapp*. In my opinion, this free-standing obligation needs to be more fully developed and extended to ensure that the detailed and nuanced reasonableness standard for third parties developed in *Ward* actually does reflect normative democratic values.

A. Legislative Context: Relationship Between Police and a Third Party

(i) *PIPEDA* and Section 487.014(1) of the *Criminal Code*

The legislative regime governing police requests for information from third parties has two intersecting components. First, section 487.014(1) of the *Criminal Code* states that police may request information from third parties without a production order, as long as the third party is not prohibited by law from disclosing that information.[43] The *Ward* Court stressed that responding to a police request for information does not in itself transform the third party into an agent of the state, especially where the ISP has its own legitimate interest in collecting the information at issue.[44] If it had collected the information at the behest of police, then the third party's conduct would have to conform to the higher standard of privacy protection that section 8 sets out for state actors and their agents. Because the third party can choose whether to provide the information it already has to police,[45] the third party's autonomy interests are implicated. Therfore, according to *Ward*, the reasonableness of its decision is informed by its "legitimate interests", as elaborated below.[46]

Second, courts in CNA cases have applied legislation governing third-party privacy obligations to determine whether the service provider was "prohibited by law" from disclosing information to police, as required by section 487.014(1) of the *Criminal Code*. Section 7(3)(c.1)(ii) of *PIPEDA* specifically permits businesses to disclose customer information upon police request without the knowledge or consent of the customer.[47] *Ward*

43. RSC 1985, c C–46, s 487.014(1).

44. *Supra* note 1 at para 96.

45. See Tim Quigley, *Procedure in Canadian Criminal Law*, loose-leaf, 2d ed (Toronto: Carswell, 2013) ch 5 at 2.1.

46. *Supra* note 1 at para 98. See also *R v Gomboc*, *supra* note 12 (describing the role of the service provider as "limited to the wholly voluntary cooperation of a potential crime victim" at para 42).

47. *Supra* note 19, s 7(3)(c.1)(ii).

went further than previous judgments, however, by stressing that to comply with *PIPEDA*, a business' voluntary disclosure to police must comply with the reasonableness standard internal to *PIPEDA*, which governs the statute as a whole.[48] According to this analysis, third-party discretion to disclose customer information upon police request under *PIPEDA* is not open-ended, but must be reasonable.

This internal reasonableness standard is stated most forcefully in section 5 of *PIPEDA*: "An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances."[49] However, this standard is not as stringent as that required of state actors by section 8, because what is reasonable for a private organization involves balancing the organization's own interests with those of its customers rather than conforming to what is normatively reasonable for state actors, as governed by the *Charter*.[50] So, while the *Ward* Court should be lauded for limiting the scope of permissible disclosure by a service provider under the *PIPEDA* regime, the statute's internal reasonableness standard is not necessarily equipped to handle the normative heavy lifting done by section 8. What if, as in *Trapp*, the governing legislation does not contain an internal reasonableness provision? In this situation, where do the normative limitations on third-party disclosure to police come from?

The governing privacy legislation in *Trapp* was Saskatchewan's *Freedom of Information and Protection of Privacy Act*.[51] This Act does not require that ISP information disclosure be reasonable. The *Trapp* Court reached for a free-standing obligation to act reasonably, regardless of the legislative context:

> It seems to me that a reasonable person, mindful of the fact such confidential and private information is potentially capable of revealing much about the online activity of the individual in the home, and mindful, too, of the obligations of [the service provider] to its

48. *Supra* note 1 at paras 45, 95–105. Compare *R v Spencer*, *supra* note 3 at paras 34–35.

49. *Supra* note 19, s 5.

50. *Ibid*, s 3 (setting out the balance in the purpose provision). See also 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 496–99.

51. SS 1990–91, c F-22.01. The relevant provision regarding disclosure to police, section 29(1)(g), is substantially similar to section 7(3)(c.1)(ii) of *PIPEDA*. *Supra* note 9, s 7(3)(c.1)(ii).

> subscribers, might reasonably expect [the service provider] to exercise a meaningful measure of independent and informed judgment before voluntarily disclosing such information to the police. This is especially so, I might add, of the reasonable and informed person concerned about the long-term consequences of government action for the protection of privacy.[52]

The Saskatchewan Court of Appeal in *Trapp* helpfully situated the third party's actions within a normative framework: the third party's actions were judged in a way akin to those of a state actor, that is, from the perspective of "the reasonable and informed person concerned about the long-term consequences of government action for the protection of privacy".[53] Unfortunately, the *Trapp* Court did not clarify how to evaluate an organization's exercise of a "meaningful measure of independent and informed judgment".[54] However, as we will see, the Ontario Court of Appeal's analysis in *Ward* of the standard of reasonableness required of private organizations under *PIPEDA* provides guidance on what such a "meaningful measure" should look like.

(ii) *Ward*'s Analysis of the *PIPEDA* Reasonableness Standard

The *Ward* Court set out explicit means to evaluate the reasonableness of a service provider's actions within *PIPEDA*.[55] Most of these factors were related to the third party's legitimate interests, which were then weighed against the privacy interests of the customer for the purposes of *PIPEDA*, though not for the purposes of the *Charter*. According to *Ward*, businesses under *PIPEDA* may consider "the nature of the investigation, and the nature of the information requested",[56] even though these same factors are off-limits for state actors as they would likely compromise the neutrality of the privacy analysis required by section 8. Thus, *Ward* turned on a distinction between the "nature of the information requested" (i.e., from the ISP's perspective) and the "subject matter of the search" (i.e., from the state's perspective) when conducting its *PIPEDA*

52. *Supra* note 2 at para 55.
53. *Ibid* at para 22, citing *R v Patrick*, 2009 SCC 17 at para 14, [2009] 1 SCR 579.
54. *Supra* note 2 at para 57.
55. *Supra* note 1 at para 105.
56. *Ibid* at para 45.

reasonableness analysis.[57] Unlike state actors, from whom information in which a person has a reasonable expectation of privacy is simply protected—for example, information that can help link a person with their internet activity on specific occasions—ISPs must assess the level of privacy protection they owe to customers based on the "sensitivity" of the information in question.

The analysis of sensitivity of information is contextual. Under *PIPEDA*, CNA information is sometimes deemed sensitive, depending on the activity with which it is associated.[58] It is therefore questionable whether the information at issue in *Ward* was truly not sensitive, even from a business perspective. That information would potentially reveal the identity of a person who committed a criminal act of a sexual nature, which seems intuitively to qualify as sensitive information. The *Ward* Court attempted to refine the analysis:

> In considering whether [the ISP] acted reasonably in disclosing the information, the nature of the information sought is relevant. The police request was specific and narrow. They sought only the client's name and address. That information in and of itself revealed nothing personal about the appellant or his Internet usage. The request was also narrow in the sense that it identified three specific instances of Internet activity. By disclosing the subscriber information to the police, [the ISP] would not be telling the police anything about the client's Internet activities at any time other than three times identified in the requests.[59]

The Court here gave weight to the fact that the ISP responded to a police request for CNA information related to specific moments in time, and hence connected to pinpointed internet activity. This is in contrast to a broader request that would potentially reveal a longer temporal window of such activity. Surely, a more general request for identifying information should weigh against the reasonableness of a decision to voluntarily disclose a customer's identity to police. Still, it remains unclear why the fact that police sought only the client's name and address did not deserve more careful handling in this context, given that these specific instances would potentially reveal that the customer had engaged in serious criminal activity (child pornography offences).

57. *Ibid* at paras 90–91.
58. *Supra* note 19, Schedule 1, s 4.3.4.
59. *Supra* note 1 at para 101.

Because the *Ward* court took a narrow view of what counts as sensitive information, a heavier burden should fall on the other factor in the business' balancing exercise: whether the legitimate interests of the business outweigh the organization's obligations regarding customer privacy. According to *Ward*, an ISP has a legitimate interest in preventing criminal misuse of its services.[60] Therefore, when weighing the balance between this interest and the obligation to protect customer privacy, an ISP may take into account the fact that police asked for CNA information about specific instances of *alleged criminal activity*. While this factor could militate *against* disclosure given the privacy interests of its customers (i.e., considering the sensitivity of the information), it clearly militates *in favour of* disclosure from the perspective of the business' legitimate interests.

Of course, the Supreme Court of Canada has repeatedly held that the fact of criminal activity does not affect the reasonableness of a defendant's expectation of privacy vis-à-vis the state.[61] However, according to *Ward*, ISPs are not required to maintain the same neutrality when considering their own interests. The distinction is that the nature and seriousness of the crime only affects the organization's interests, not the customer's. Serious crimes committed via an ISP's services have a more dramatic effect on the interests of the service provider, making the decision to disclose more reasonable.[62] The nature and seriousness of the offence and the fact that a defendant attempted to conceal the criminal activity are

60. *Ibid* at para 97.

61. See *R v Wong*, *supra* note 38 at 50–51 (a defendant's expectation of privacy in a hotel room is not altered by the illegal activity going on there); *R v Kang-Brown*, 2008 SCC 18 at para 100, [2008] 1 SCR 456 (a defendant's expectation of privacy in a closed bag is not altered by the fact that marijuana is concealed within it); *R v Patrick*, *supra* note 53 ("[a] warrantless search of a private place cannot be justified by the after-the-fact discovery of evidence of a crime" at para 32).

62. The "seriousness of the offence" was initially listed among the factors courts should consider when determining whether the defendant's expectation of privacy was reasonable. *R v Plant*, *supra* note 12 at 295. However, the Supreme Court in *R v Tessling* relocated this factor to the second stage of the section 8 inquiry and to the inquiry under section 24(2) of the *Charter*—that is, whether the search was reasonable and whether the evidence should be excluded, respectively. 2004 SCC 67 at para 64, [2004] 3 SCR 432. See also Daniel Michaluk, "ISP Disclosure Decision Touches Deep Questions About Anonymity, Third Party Interests" (3 October 2012), online: All About Information <http://allaboutinformation.ca>.

not directly relevant to the defendant's expectation of privacy vis-à-vis the state. Nonetheless, these factors can indirectly reduce the reasonableness of that expectation, since they inform a business' assessment of its own interests.

In several of the CNA cases, ISPs (including Bell Canada) have stated that they will generally only disclose account holder information without a warrant in the furtherance of online child exploitation investigations.[63] Such a policy can meet the standard of reasonableness applicable to private actors set out in *Ward*, for two reasons. First, online child exploitation offences make integral use of the ISP's services, so they directly invoke its legitimate interest in preventing those services from being criminally misused.[64] Second, *Ward* acknowledged participation in crime control more generally as a legitimate interest, so a service provider can also take into consideration its capacity to assist in the control of crimes that target vulnerable members of society.

Offences involving the abuse of children most often result from violated trust relationships. Consequently, non-state actors, especially those well-placed to assist, have regularly been enlisted in protecting children against abuse.[65] ISPs have responded to this strong social imperative by being willing to assist in online child-exploitation investigations. Unlike *Charter*-regulated state actors, non-state actors can legitimately be informed by such social imperatives because they are required to consider their own legitimate interests rather than those of the society at large.[66]

63. See *R v Cuttell*, *supra* note 7 at para 8; *R v Brosseau*, *supra* note 7 at para 42.

64. Emphasis on self-protection (for individuals and businesses) and private property owners' obligations to reduce criminal opportunities are aspects of the new perception of effective crime prevention. See e.g. David H Bayley, *Police for the Future* (Oxford: Oxford University Press, 1994) at 108–11. For an internet-specific discussion, see generally Bradford W Reyns, "A Situational Crime Prevention Approach to Cyberstalking Victimization: Preventative Tactics for Internet Users and Online Place Managers" (2010) 12:2 Crime Prevention and Community Safety 99.

65. See Wayne N Renke, "The Mandatory Reporting of Child Abuse Under the Child Welfare Act" (1999) 7 Health LJ 91 at 112. See also Slane & Austin, *supra* note 50 at 491–95.

66. But see *R v Spencer*, *supra* note 3. The *Spencer* Court raised some concerns about this type of distinction, stating that "given the nature of the offences alleged, a reasonable person might consider [the service provider's] disclosure of the Disclosed Information to have been 'appropriate in the circumstances', but that simple analysis would ignore the fundamental principle of the presumption of innocence, among other things". *Ibid* at para 35. The *Ward* Court was attempting to distinguish its analysis from such a "simple analysis".

Against this backdrop, the Court in *Ward* denied falling into "the trap of judging the appellant's privacy expectation by reference to the nature of his activity".[67] The Court reiterated that

> [t]he nature of the offence under investigation is relevant to the reasonableness of [the ISP's] response to the police request. The nature of the activity that would actually be revealed to the police by the information provided by [the ISP] is not germane to the reasonable expectation of privacy inquiry.[68]

In other words, *Ward* gave weight to the autonomous interests of the third party *as* a third party, insofar as these interests inform what is reasonable disclosure *for* a third party who is charged with weighing the competing interests of its customers with its own. However, no matter how different the approach may be for a private actor under privacy legislation, it is open to question whether it comports with the normative underpinnings of section 8. I will return to this question below.

B. Contractual Context: Relationship Between a Third-Party Service Provider and a Defendant

The Court in *Ward* emphasized that contractual terms are relevant to, but not determinative of, the reasonableness of a person's expectation of privacy. The Court thereby rejected the reasoning used in some trial-level cases, which treated the content of service agreements as nearly wholly determinative of whether a customer's expectation of privacy in his account information was reasonable.[69] As well, *Ward* noted that because a service agreement is a classic contract of adhesion, it has limited value as an expression of the customer's express consent to its specific terms.[70] Despite this, the *Ward* Court found it relevant that the ISP service agreement and related documents clearly stated that using the services to engage in child pornography offences was contrary to the ISP's Acceptable Use

67. *Supra* note 1 at para 103.
68. *Ibid.*
69. See e.g. *R v Cuttell*, *supra* note 7 at paras 28–30 (citing other recent cases with approval to the effect that contractual terms can exert considerable weight against a reasonable expectation of privacy).
70. *Supra* note 1 at para 52.

Policy (AUP).[71] The agreement also expressly noted the ISP's willingness to "offer full co-operation with law enforcement agencies in connection with any investigation arising from a breach of this AUP".[72] Because of this degree of specificity, the Court found that the contract weighed against the reasonableness of the defendant's expectation of privacy.

However, many ISP service agreements and AUPs, including those at issue in *Ward*, state that ISPs are willing to cooperate with police in *any* breach of the agreement, which can include a broad array of specified and unspecified misuses.[73] Additionally, not all service agreements explicitly state what sort of customer information the ISP is willing to share with police.[74] In *Ward*, the service agreement broadly reserved the ISP's right to disclose any information "necessary to satisfy any laws, regulations, or other governmental request" and to "offer full cooperation with law enforcement agencies in connection with any investigation arising from a breach of this AUP".[75] Such broad terms, if taken at face value, would mean that the customer would have virtually no expectation of privacy left. While the *Ward* Court did not explicitly say so, it appears to have applied a reasonableness standard like that developed under *PIPEDA* to interpret the contractual terms. As the Court wrote in *Ward*:

> I stress that the conclusion in this case is based on the specific circumstances revealed by this record and is not intended to suggest that disclosure of customer information by an ISP can never infringe the customer's reasonable expectation of privacy. If, for example, the ISP disclosed more detailed information, or made the disclosure in relation to an investigation of an offence in which the service was not directly implicated, the reasonable expectation of privacy analysis might yield a different result.[76]

71. *Ibid* at para 54.
72. *Ibid* at para 56.
73. See *supra* note 1 at para 56. See also *R v Ward*, 2008 ONCJ 355, 176 CRR (2d) 90 (while the service agreement that the defendant entered into with his ISP included specific mention of child pornography offences, it also prohibited customers from "[t]ransmitting, posting, receiving, retrieving, storing or otherwise reproducing, distributing or providing access to any program or information constituting or encouraging conduct that would constitute a criminal offence or give rise to civil liability" at para 45).
74. See *R v Ward*, *supra* note 1 at para 107.
75. *Ibid* at para 55.
76. *Ibid* at para 109.

This aspect of the judgment needs further development. However, it appears to indicate that while the terms of a contract can weigh against the reasonableness of a defendant's expectation of privacy if they explicitly address the circumstances at issue in the case, those terms must nonetheless be normatively reasonable. In other words, in cases of this sort, only legitimate business interests can be weighed against a service provider's obligation to guard its customers' privacy. Thus, broad statements of willingness to cooperate with law enforcement officials set out in many service agreements would essentially apply only where the information requested was relatively narrow and specific to a criminal offence which directly implicates the service or facilities of the business.[77] In my reading of the judgment, the Court envisaged giving less weight to overly broad contractual terms, so that terms of service contracts and related documents cannot completely defeat a customer's claim to information privacy, even where they say so in plain language.

Taken together, *Ward*'s analysis of the legislative and contractual contexts helps to set principled limits on the circumstances in which a third-party service provider's decisions to disclose CNA information can negate a defendant's reasonable expectation of privacy in that information. However, these constraints are mostly based on a specific legislative regime, *PIPEDA*, and cannot reflect a truly normative approach because the Act does not apply to all custodians of customer information. Nonetheless, the *Ward* Court supported the idea, set out by the Saskatchewan Court of Appeal in *Trapp*, that "the reasonable expectation of privacy inquiry must proceed on the basis that the service provider will exercise a 'meaningful measure of independent and informed judgment' in deciding whether to make the disclosure requested by the police".[78] This idea is independent of the specific legislative context, so it undergirds the normative inquiry more broadly. The *Ward* Court's analysis of reasonableness under *PIPEDA* appears to serve as an *example* of what *Trapp* called a "meaningful measure", but this requirement of a meaningful measure should not disappear in the absence of a specific statute.

77. See *Criminal Code*, *supra* note 43 (defining the offence of possession of child pornography as "knowingly caus[ing] child pornography to be viewed by, or transmitted to, himself or herself", s 163.1(4.2)).

78. *Supra* note 1 at para 105, citing *supra* note 2 at para 55.

For a deeper investigation of whether *Ward* adequately addressed the normative underpinning of the section 8 analysis, I will now turn to the historical context of what criminologist David Garland calls the "new culture of crime control".[79] I will argue that *Ward*'s third-party mediated analysis—placing limits on the impact of third-party interests on the defendant's privacy rights—is a step in the right direction given this context, but that more clarification is needed to truly reflect the values underlying a democratic society.

III. New Culture of Crime Control: ISP Self-Interest and Civic Engagement in the Information Age

A. The Rise of the New Culture of Crime Control

Businesses have long had an interest in preventing criminal misuse of their services and facilities, both to protect themselves against criminal victimization and to maintain a reputation for trustworthiness. Situational crime prevention is a contemporary model of policing that exhorts businesses to be particularly vigilant in this area and pushes for broader civic engagement in the collective project of crime control. According to Garland, starting in the 1960s researchers used new methods of collecting criminological research data—self-report studies, victim surveys and interviews with offenders—with a view to providing evidence of "[t]he normality of crime and the generality of deviance."[80] Before that, crime was considered a problem to be confined to certain sub-populations who could be contained or cured of deviance. The new perspective sees crime as a pervasive and persistent problem that law enforcement will never be able to eradicate fully.[81]

When combined with cost control measures in the public sector, this shift toward a perception of permanent criminality has led police and prosecutors to prioritize their crime control activities (e.g., to focus

79. David Garland, "Ideas, Institutions and Situational Crime Prevention" in Andrew von Hirsch, David Garland & Alison Wakefield, eds, *Ethical and Social Perspectives on Situational Crime Prevention* (New York: Oxford University Press, 2000) 1 at 11.

80. *Ibid* at 12.

81. See *ibid*.

mainly on major crimes). Increasingly they emphasize that the public must take measures to protect itself from criminal activity, both individually and collectively.[82] Together, these changes have resulted in the rise of the private security industry and in policy-makers extolling situational crime prevention as common sense.[83] One principle of situational crime prevention is that crime can be reduced by increasing potential criminals' perceptions that a criminal act is risky—i.e., that the perpetrator is likely to get caught.[84] From this perspective, businesses patrolling their own properties help to make up for the lack of available resources for more widespread surveillance, and thereby share with police the burden of reducing crimes that directly affect them.[85]

B. ISPs in the New Culture of Crime Control

The difficulty in policing online crime has become a central theme in scholarship and public debate, especially with respect to the technical expertise required to identify and locate offenders.[86] Because the private sector is widely perceived as far more technologically sophisticated than the police, ISPs were in effect "responsibilized" (made responsible for) their own network security.[87] As such, the internet is in effect "policed" by a

82. *Ibid.*

83. *Ibid* at 12–13.

84. See RVG Clarke, "'Situational' Crime Prevention: Theory and Practice" (1980) 20:2 Brit J Crim 136 at 138; Marcus Felson, *Crime and Everyday Life*, 3d ed (Thousand Oaks, Cal: Sage Publications, 2002) at 146.

85. The shift to community partnerships and private security is frequently criticized by scholars as a negative development; they see these social changes as contributing to a "surveillance society" that compromises civil liberties. See e.g. Alison Wakefield, "The Public Surveillance Functions of Private Security" (2005) 2:4 Surveillance & Society 529.

86. See e.g. David S Wall, "The Internet as a Conduit for Criminal Activity" in April Pattavina, ed, *Information Technology and the Criminal Justice System* (Thousand Oaks, Cal: Sage, 2005) 77; Johnny Nhan & Laura Huey, "Policing Through Nodes, Clusters and Bandwidth" in Stéphane Leman-Langlois, ed, *Technocrime: Technology, Crime and Social Control* (Cullompton, UK: Willan Publishing, 2008) 66; Laura J Huey, "Policing the Abstract: Some Observations on Policing Cyberspace" (2002) 44:3 Can J Crim 243; Neal Kumar Katyal, "Digital Architecture as Crime Control" (2003) 112:8 Yale LJ 2261.

87. See generally David S Wall, "Policing Cybercrimes: Situating the Public Police in Networks of Security Within Cyberspace" (2007) 8:2 Police Practice and Research 183.

wide variety of actors, many of them private.[88] This sort of public-private partnership—whether formal or informal—has a far-reaching appeal which goes beyond the self-interested aspect of participation in crime control.

Situational crime prevention encourages citizens and community organizations to participate in crime control.[89] When combined with the "responsibilization" of private actors, this shift helps to explain how, in the last thirty years, child protection advocates have successfully lobbied the government to extend responsibility for child welfare beyond the confines of the family.[90] Many jurisdictions, including Canada, now mandate the reporting of suspected child abuse to authorities and regularly call on the community to protect children from harm. Mandatory ISP reporting requirements for suspected child pornography offences have recently expanded the communal obligation to protect children into the online realm as well.[91]

During the early days of the internet, ISPs were eager to avoid regulation as they developed business models to capitalize on rapidly unfolding technological opportunities. Self-regulation thus came to include self policing and willingness to assist law enforcement, as an alternative to government regulation.[92] Law enforcement regularly asked ISPs for help in dealing with child exploitation crimes involving their services—crimes that inspired significant social anxiety and put public pressure on

88. *Ibid.*

89. See Lorraine Mazerolle & Janet Ransley, *Third Party Policing* (New York: Cambridge University Press, 2005) ("third party policing is the use of a range of civil, criminal and regulatory rules and laws to engage (or force) third parties into taking some crime control responsibility" at 3).

90. Slane & Austin, *supra* note 50 at 491–95.

91. See *An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service*, SC 2011, c 4.

92. The Canadian Association of Internet Providers (CAIP), for instance, was a strong advocate of self-regulation, in the matter (among others) of cooperation with law enforcement requests (CAIP has since been subsumed under the CATA Alliance). For a discussion of CAIP's voluntary self-regulatory principles, see Sara M Smyth, "Mind the Gap: a New Model for Internet Child Pornography Regulation in Canada" (2007) 4:1–2 University of Ottawa Law and Technology Journal 59 at 75–76.

ISPs to cooperate with police.[93] This pressure led to the collaborative development of the "letter of request" protocol used in the CNA cases.[94] At the same time, however, customers became more concerned with the protection of personal information in the information age, as was reflected in the enactment of *PIPEDA* in 2000. Together, these historical shifts help explain why many ISPs would explicitly signal a willingness to cooperate with police when customers violated service agreements.

Through their service agreements, therefore, the large Canadian ISPs sought to assure customers that they take information protection seriously, to tell customers that they intend to maintain internal security and powers of investigation for crimes that affect ISPs, and to publicly signal their enthusiastic participation in crime control in order to show that corporate responsibility makes government regulation of the industry unnecessary. The message to customers is that if they do not approve of this mix of purposes, they should move to a different ISP.[95]

Social norms have no doubt evolved to encourage third parties to participate in crime control, but it is not clear how these social changes can most appropriately be incorporated into the normative approach to section 8 that the *Ward* Court insisted was needed.[96] I turn to this issue for the remainder of the comment.

93. See e.g. "Every Image, Every Child: Internet-Facilitated Child Sexual Abuse in Canada" (2007–08), online: Office of the Federal Ombudsman for Victims of Crime <http://www.victimsfirst.gc.ca> at 40–42.

94. As noted earlier, the letter of request is the simplified form letter ISPs and police agreed to use for CNA information requests in child exploitation investigations. For an account of the development of the letter of request protocol, see Slane & Austin, *supra* note 50 at 488–90.

95. Note that all of the major Canadian ISPs—Bell, Rogers, Shaw, Cogeco and Telus—were members when the Canadian Coalition Against Internet Child Exploitation crafted the letter of request protocol. CAIP represented some but not all smaller ISPs. See "Canadian Coalition Against Internet Child Exploitation (CCAICE) National Action Plan Highlights", online: cybertip.ca <https://www.cybertip.ca>.

96. Lisa Austin sets out the useful distinction in section 8 jurisprudence between truly normative standards of reasonableness and standards reflecting social conventions. She notes that the danger in a social conventions approach is that its content is not normative. She prefers the "independent justification approach" rooted in democratic principles. Lisa M Austin, "Privacy and the Question of Technology" (2003) 22:2 Law & Phil 119 at 142–43. See also James AQ Stringham, "Reasonable Expectations Reconsidered: A Return to the Search for a Normative Core of Section 8?" (2005) 23 CR (6th) 245 (adopting Austin's distinction).

IV. Establishing Normative Values When Third Parties Mediate the Relationship Between Police and Defendants

In *Ward*, the Ontario Court of Appeal attempted to articulate the normative underpinning for crime control participation of private actors:

> The normative nature of the reasonable expectation of privacy analysis and the value judgments that underlie that analysis require that [the service provider's] legitimate interests, whether described as self-interest, civic engagement, or both, be taken into account in determining whether the appellant had a reasonable expectation of privacy in respect of the information held by [the ISP]. A reasonable and informed person considering whether society would find it reasonable for the appellant to have a reasonable expectation of privacy in his subscriber information would take into account [the ISP's] legitimate interests in voluntarily disclosing that information to the police when that disclosure would assist in an investigation of the alleged criminal misuse of [the ISP's] services, assuming the disclosure was not prohibited and would not violate any laws or the terms of applicable customer agreement.[97]

By stating that a normative analysis must consider the third party's "legitimate interests" in participating in crime control, *Ward* validated the current historical context—the new culture of crime control. However, the above passage is very ambiguous on how taking these interests into account comports with a truly normative approach—one that follows from what Lisa Austin has called an "independent justification for privacy" based on democratic values that are more durable than (and hence distinct from) mere social conventions.[98]

This issue of the extent to which ISP cooperation with police would be *Charter*-compliant is a complicated one. Social change sometimes requires adjustments to the normative values used to determine where and how "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".[99] Many privacy advocates are understandably concerned about expansion of the role of non-state actors in the evolving crime control approach, especially because

97. *Supra* note 1 at para 98.
98. *Supra* note 96 at 136.
99. *Southam*, *supra* note 37 at 159–60.

the *Charter* does not directly govern third parties.[100] Many commentators have argued that the internet poses particularly strong risks to privacy because of the massive amounts of personal data that travel through and are stored on privately-owned networks.[101] The stakes are therefore high for the future of online privacy protections afforded by the *Charter*, and it is important that we get right the normative assessment of the role of voluntary cooperation of ISPs with public authorities.

To substantiate the conclusion that it is normatively sound to take ISPs' legitimate interests into consideration, the *Ward* Court drew on the Supreme Court of Canada's reasons in *Tessling*, which included the assertion that the "expectation of privacy is a normative rather than a descriptive standard".[102] Justice Doherty, writing for the Court in *Ward*, elaborated as follows:

> By "normative", I understand Binnie J [in *Tessling*] to mean that in determining whether an individual enjoys a reasonable expectation of privacy, the court is making a value judgment more than a finding of fact in the traditional sense. When the court accepts the contention that a person has a reasonable expectation of privacy, the court is in reality declaring that the impugned state conduct has reached the point at which the values underlying contemporary Canadian society dictate that the state must respect the personal privacy of individuals unless it is able to constitutionally justify any interference with that personal privacy.[103]

One way to reconcile third-party interests with a normative approach of this sort would be to consider the balancing exercise as a whole to be

100. Privacy advocates have criticized Bill C-12 as an "anti-privacy privacy bill" because it would appear to expand the scope of voluntary cooperation with police investigations. *Safeguarding Canadians' Personal Information Act*, 1st Sess, 41st Parl, 2011. See British Columbia Civil Liberties Association et al, "Open letter to the House of Commons Standing Committee on Access to Information, Privacy and Ethics" (19 November 2010), online: Canadian Internet Policy and Public Internet Clinic <http://www.cippic.ca>.

101. See Arthur J Cockfield, "Who Watches the Watchers? A Law and Technology Perspective on Government and Private Sector Surveillance" (2003) 29:1 Queen's LJ 364; Laura Huey & Richard S Rosenberg, "Watching the Web: Thoughts on Expanding Police Surveillance Opportunities Under the Cyber-Crime Convention" (2004) 46:5 Canadian Journal of Criminology and Criminal Justice 597. See generally David Lyon, *The Electronic Eye: The Rise of Surveillance Society* (Minneapolis: University of Minnesota Press, 1994).

102. *Supra* note 1 at para 81, citing *supra* note 62 at para 42.

103. *Supra* note 1 at para 82.

governed by "the values underlying contemporary Canadian society",[104] and not just by the values that protect individuals from unreasonable state intrusion. In other words, underlying social values do not serve only to constrain government intrusion in order to maintain a free, democratic and open society; they also serve to inform when it is reasonable to *permit* state intrusions in the interests of such a society.

The *Ward* Court drew support for the permissive aspect of normative reasonableness in the area of privacy interests from the Supreme Court's reasons in *R v Patrick*, which included the statement that "[p]rivacy analysis is laden with value judgments which are made from the independent perspective of the reasonable and informed person who is concerned about the long-term consequences of government action for the protection of privacy."[105] In other words, the government action that "society is prepared to recognize as 'reasonable'"[106] is informed both by the values that protect privacy and those that support law enforcement intrusion when appropriate. From this perspective, third-party interests can figure into the values supporting effective law enforcement where a third party's services or facilities are directly implicated in such enforcement.

This is, however, only one way of thinking about the normative placement of third-party actions in relation to the *Charter*, and it carries with it the risk of confusing social conventions—what we have come to accept as normal—with the deeper normative values underlying the right to privacy in a democratic society. Elsewhere in its judgment, the *Ward* Court said that the section 8 inquiry is about "whether the appellant has a reasonable expectation that he could anonymously access the Internet on his computer without the state, with the cooperation of the appellant's ISP, being able to find out what he had accessed".[107] I contend that it is not only the legitimate interests of the ISP that come into play in regulating the process whereby the state, with the cooperation of the appellant's ISP, gains access to a defendant's personal information. Also in issue in determining whether a business has acted reasonably is the balance that the business must strike between those interests and the privacy interests

104. *Ibid*.

105. *Ibid* at para 84, citing *R v Patrick*, *supra* note 53 at para 14.

106. *R v Ward*, *supra* note 1 at para 86, citing *R v AM*, *supra* note 12 at para 33.

107. *Supra* note 1 at para 88.

of its customers. A free-standing requirement of such a balance in the third party's decision making would be a normative measure, certainly more so than one which took only the business' interests into account.

As noted above, the Saskatchewan Court of Appeal in *Trapp* indicated the need for a free-standing obligation on third parties to protect customer privacy when considering police requests:

> [T]he reasonable person might well think that [the ISP] does not enjoy an unfettered discretion to divulge confidential information to others—unfettered, that is, beyond the prerequisite of being "legally empowered" to do so. Otherwise, the information loses much if not all of its confidential character. And the element of confidentiality in the relationship is substantially compromised. So, the reasonable person might well think that [the ISP] would be highly circumspect when it comes to divulging to others confidential information of the nature and quality of the information in question.[108]

By invoking the reasonable person in this way, *Trapp* suggested that the *Charter*'s deeper normative standard imposes an obligation on third parties to give central consideration to customer privacy when deciding that whether to disclose customer information to police. However, while that suggestion is helpful, the *Trapp* decision does not provide sufficient guidance to third parties faced with such a decision. I suggest that the balancing approach in *Ward* does provide this needed guidance. That is, a free-standing requirement of reasonableness in third-party decision making—appropriately balancing customer privacy with legitimate business interests—holds more promise as a means of achieving a truly normative assessment of the circumstances in the first prong of the section 8 analysis in a given case.

Conclusion

If we incorporate a free-standing reasonableness requirement for third-party cooperation with police into the section 8 analysis as a whole, we will be better equipped to ensure that the new culture of crime control reflects the normative values appropriate to a free and democratic society. *Ward* gets us some distance toward that goal. Perhaps in *Spencer*, the Supreme Court will complete the journey.

108. *Supra* note 2 at para 47.