R. *v.* SPENCER, 2014 SCC 43, December 9; 2014 (Cromwell J. delivered the opinion)

I. Introduction

[1] The Internet raises a host of new and challenging questions about privacy. This appeal relates to one of them.

[2] The police identified the Internet Protocol (IP) address of a computer that someone had been using to access and store child pornography through an Internet file-sharing program. They then obtained from the Internet Service Provider (ISP), without prior judicial authorization, the subscriber information associated with that IP address. This led them to the appellant, Mr. Spencer. He had downloaded child pornography into a folder that was accessible to other Internet users using the same file-sharing program. He was charged and convicted at trial of possession of child pornography and acquitted on a charge of making it available.

[3] At trial, Mr. Spencer claimed that the police had conducted an unconstitutional search by obtaining subscriber information matching the IP address and that the evidence obtained as a result should be excluded. He also testified that he did not know that others could have access to the shared folder and argued that he therefore did not knowingly make the material in the folder available to others. The trial judge concluded that there had been no breach of Mr. Spencer's right to be secure against unreasonable searches and seizures. However, he was of the view that the "making available" offence required some "positive facilitation" of access to the pornography, which Mr. Spencer had not done, and further he believed Mr. Spencer's

evidence that he did not know that others could access his folder so that the fault element (*mens rea*) of the offence had not been proved. The judge therefore convicted Mr. Spencer of the possession offence, but acquitted him of the making available charge.

[4] The Court of Appeal upheld the conviction for possession of child pornography, agreeing with the trial judge that obtaining the subscriber information was not a search and holding that even if it were a search, it would have been reasonable. The court, however, set aside the acquittal on the making available charge on the basis that the trial judge had been wrong to require proof of positive facilitation of access by others to the material. A new trial was ordered on this charge.

The appeal to this Court raises four issues which I would resolve as follows:

1. Did the police obtaining the subscriber information matching the IP address from the ISP constitute a search?

   In my view, it did.

2. If so, was the search authorized by law?

   In my view, it was not.

   . . .

II. Analysis

A. *Did the police obtaining the subscriber information matching the IP address from the ISP constitute a search?*

[5] Mr. Spencer maintains that the police were conducting a search when they obtained the subscriber information associated with the IP address from the ISP, Shaw Communications Inc. The respondent Crown takes the opposite view. I agree with Mr. Spencer on this point. I will first set out a summary of the relevant facts then turn to the legal analysis.

(1) Facts and Judicial History

[6] Mr. Spencer, who lived with his sister, connected to the Internet through an account registered in his sister's name. He used the file-sharing program LimeWire on his desktop computer to download child pornography from the Internet. LimeWire is a free peer-to-peer file-sharing program that, at the time, anyone could download onto their computer. Peer-to-peer systems such as LimeWire allow users to download files directly from the computers of other users. LimeWire does not have one central database of files, but instead relies on its users to share their files directly with others. It is commonly used to download music and movies and can also be used to download both adult and child pornography. It was Mr. Spencer's use of the file-sharing software that brought him to the attention of the police and which ultimately led to the search at issue in this case.

[7] Det. Sgt. Darren Parisien (then Cst.) of the Saskatoon Police Service, by using publicly available software, searched for anyone sharing child pornography. He

could access whatever another user of the software had in his or her shared folder. In other words, he could "see" what other users of the file sharing software could "see". He could also obtain two numbers related to a given user: the IP address that corresponds to the particular Internet connection through which a computer accesses the Internet at the time and the globally unique identifier (GUID) number assigned to each computer using particular software. The IP address of the computer from which shared material is obtained is displayed as part of the file-sharing process. There is little information in the record about the nature of IP addresses in general or the IP addresses provided by Shaw to its subscribers. There is a description in *R. v. Ward*, 2012 ONCA 660, 112 O.R. (3d) 321, at paras. 21-26 which also notes some of differences that may exist among IP addresses. For the purposes of this case, what we know is that the IP address obtained by Det. Sgt. Parisien matched computer activity at the particular point in time that he was observing that activity.

[8] Det. Sgt. Parisien generated a list of IP addresses for computers that had shared what he believed to be child pornography. He then ran that list of IP addresses against a database which matches IP addresses with approximate locations. He found that one of the IP addresses was suspected to be in Saskatoon, with Shaw as the ISP.

[9] Det. Sgt. Parisien then determined that Mr. Spencer's computer was online and connected to LimeWire. As a result, he (along with any LimeWire user) was able to browse the shared folder. He saw an extensive amount of what he believed to be child pornography. What he lacked was knowledge of where exactly the computer was and who was using it.

[10] To connect the computer usage to a location and potentially a person, investigators made a written "law enforcement request" to Shaw for the subscriber information including the name, address and telephone number of the customer using that IP address. The request, which was purportedly made pursuant to s. 7(3)(*c.1*)(ii) of the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 (*PIPEDA*), indicated that police were investigating an offence under the *Criminal Code*, R.S.C. 1985, c. C-46, pertaining to child pornography and the Internet and that the subscriber information was being sought as part of an ongoing investigation. (The full text of the relevant statutory provisions is set out in an Appendix.) Investigators did not have or try to obtain a production order (i.e. the equivalent of a search warrant in this context).

[11] Shaw complied with the request and provided the name, address and telephone number of the customer associated with the IP address, Mr. Spencer's sister. With this information in hand, the police obtained a warrant to search Ms. Spencer's home (where Mr. Spencer lived) and seize his computer, which they did. The search of Mr. Spencer's computer revealed hundreds of child pornography images and over a hundred child pornography videos in his shared LimeWire folder.

[12] Mr. Spencer was charged with possessing child pornography contrary to s. 163.1(4) of the *Criminal Code* and making child pornography available over the Internet contrary to s. 163.1(3). There is no dispute that the images found in his shared folder were child pornography.

[13] At trial, Mr. Spencer sought to exclude the evidence found on his computer on the basis that the police actions in obtaining his address from Shaw without prior judicial authorization amounted to an unreasonable search contrary to s. 8 of the *Canadian Charter Rights and Freedoms*. The trial judge rejected this contention and convicted Mr. Spencer of the possession count. On appeal, the Saskatchewan Court of Appeal upheld the judge's decision with respect to the search issue.

(2) Was the Request to Shaw a Search?

[14] Under s. 8 of the *Charter*, "[e]veryone has the right to be secure against unreasonable search or seizure." This Court has long emphasized the need for a purposive approach to s. 8 that emphasizes the protection of privacy as a prerequisite to individual security, self-fulfilment and autonomy as well as to the maintenance of a thriving democratic society: *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145, at pp. 156-57; *R. v. Dyment*, [1988] 2 S.C.R. 417, at pp. 427-28; *R. v. Plant*, [1993] 3 S.C.R. 281, at pp. 292-93; *R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432, at paras. 12-16; *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, 2013 SCC 62, [2013] 3 S.C.R. 733, at para. 22.

[15] The first issue is whether this protection against unreasonable searches and seizures was engaged here. That depends on whether what the police did to obtain the subscriber information matching the IP address was a search or seizure within the meaning of s. 8 of the *Charter.* The answer to this question turns on whether, in the

totality of the circumstances, Mr. Spencer had a reasonable expectation of privacy in the information provided to the police by Shaw. If he did, then obtaining that information was a search.

[16] We assess whether there is a reasonable expectation of privacy in the totality of the circumstances by considering and weighing a large number of interrelated factors. These include both factors related to the nature of the privacy interests implicated by the state action and factors more directly concerned with the expectation of privacy, both subjectively and objectively viewed, in relation to those interests: see, e.g., *Tessling*, at para. 38; *Ward*, at para. 65. The fact that these considerations must be looked at in the "totality of the circumstances" underlines the point that they are often interrelated, that they must be adapted to the circumstances of the particular case and that they must be looked at as a whole.

[17] The wide variety and number of factors that may be considered in assessing the reasonable expectation of privacy can be grouped under four main headings for analytical convenience: (1) the subject matter of the alleged search; (2) the claimant's interest in the subject matter; (3) the claimant's subjective expectation of privacy in the subject matter; and (4) whether this subjective expectation of privacy was objectively reasonable, having regard to the totality of the circumstances: *Tessling*, at para. 32; *R. v. Patrick*, 2009 SCC 17, [2009] 1 S.C.R. 579, at para. 27; *R. v. Cole*, 2012 SCC 53, [2012] 3 S.C.R. 34, at para. 40. However, this is not a purely factual inquiry. The reasonable expectation of privacy standard is normative rather than simply descriptive: *Tessling*, at para. 42. Thus, while the analysis is sensitive to

the factual context, it is inevitably "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": *Patrick*, at para. 14; see also *R. v. Gomboc*, 2010 SCC 55, [2010] 3 S.C.R. 211, at para. 34, and *Ward*, at paras. 81-85.

[18] I can deal quite briefly with two aspects of the appeal. The trial judge in this case held that there was no subjective expectation of privacy in this case: 2009 SKQB 341, 361 Sask. R. 1, at para. 18. However, as I will explain below, the trial judge reached this conclusion by incorrectly defining the subject matter of the search. On the proper understanding of the scope of the search, Mr. Spencer's subjective expectation of privacy in his online activities can readily be inferred from his use of the network connection to transmit sensitive information: *Cole*, at para. 43. Mr. Spencer's direct interest in the subject matter of the search is equally clear. Though he was not personally a party to the contract with the ISP, he had access to the Internet with the permission of the subscriber and his use of the Internet was by means of his own computer in his own place of residence.

[19] The main dispute in this case thus turns on the subject matter of the search and whether Mr. Spencer's subjective expectation of privacy was reasonable. The two circumstances relevant to determining the reasonableness of his expectation of privacy in this case are the nature of the privacy interest at stake and the statutory and contractual framework governing the ISP's disclosure of subscriber information.

[20] In this case, I have found it helpful to look first at the subject matter of the search, then at the nature of the privacy interests implicated by the state actions and then finally at the governing contractual and statutory framework. While these subjects are obviously interrelated, approaching the analysis under these broad headings provides a degree of focus while permitting full examination of the "totality of the circumstances".

(a) *The Subject Matter of the search*

[21] Mr. Spencer alleges that the police request to Shaw is a state action that constitutes a search or seizure for the purposes of s. 8 of the *Charter*. We must therefore consider what the subject matter of that request was in order to be able to identify the privacy interests that were engaged by it.

[22] In many cases, defining the subject matter of the police action that is alleged to be a search is straightforward. In others, however, it is not. This case falls into the latter category. The parties and the courts below have markedly divergent perspectives on this important issue, a divergence which is reflected in the jurisprudence: see, for example, the authorities reviewed in *Ward*, at para. 3.

[23] Mr. Spencer contends that the subject matter of the alleged search was core biographical data, revealing intimate and private information about the people living at the address provided by Shaw which matched the IP address. The Crown, on the other hand, maintains that the subject matter of the alleged search was simply a name, address and telephone number matching a publicly available IP address.

[24] These divergent views were reflected in the decisions of the Saskatchewan courts. The trial judge adopted the Crown's view that what the police sought and obtained was simply generic information that does not touch on the core of Mr. Spencer's biographical information. Ottenbreit J.A. in the Court of Appeal was of largely the same view. For him, the information sought by the police in this case simply established the identity of the contractual user of the IP address. The fact that this information might eventually reveal a good deal about the activity of identifiable individuals on the Internet was, for him, "neither here nor there": 2011 SKCA 144, 377 Sask. R. 280, at para. 110. (see also *R. v. Trapp*, 2011 SKCA 143, 377 Sask. R. 246, at paras. 119-24 and 134.) In contrast to this approach, Caldwell J.A. (Cameron J.A. concurring on this point) held that in characterizing the subject matter of the alleged search, it is important to look beyond the "mundane" subscriber information such as name and address (para. 22). The potential of that information to reveal intimate details of the lifestyle and personal choices of the individual must also be considered: see also *Trapp*, *per* Cameron J.A., at paras. 33-37.

[25] I am in substantial agreement with Caldwell and Cameron JJ.A. on this point. While, in many cases, defining the subject matter of the search will be uncontroversial, in cases in which it is more difficult, the Court has taken a broad and functional approach to the question, examining the connection between the police investigative technique and the privacy interest at stake. The Court has looked at not only the nature of the precise information sought, but also at the nature of the information that it reveals.

[26] A number of decisions of the Court reflect this approach. I begin with *Plant*. There, the Court, dealing with informational privacy, stressed the strong claim to privacy in relation to information that is at the "biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state": p. 293. Importantly, the Court went on to make clear that s. 8 protection is accorded not only to the information which is itself of that nature, but also to "information which tends to reveal intimate details of the lifestyle and personal choices of the individual": *ibid.* (emphasis added).

[27] *Tessling* took the same approach, although it led to a different conclusion. The subject matter of the alleged search was held to be the heat emitted from the surface of a building. The Forward Looking Infra-Red (FLIR) imaging technique was used to help assess the activities that transpired inside a house, but the heat emissions by themselves could not distinguish between one heat source and another. In short, the heat emanations were, on their own, meaningless because they did not permit any inferences about the precise activity giving rise to the heat: paras. 35-36. The critical question was: what inferences about activity inside the home — admittedly a highly private zone — did the FLIR images support?

[28] I turn next to *R. v. Kang-Brown*, 2008 SCC 18, [2008] 1 S.C.R. 456, and the companion appeal in *R. v. A.M.*, 2008 SCC 19, [2008] 1 S.C.R. 569. While the Court divided on other points, it was unanimous in holding that the dog sniff of Mr. Kang-Brown's bag constituted a search. As explained by both Deschamps and Bastarache JJ., the dog sniffing at the air in the vicinity of the bag functioned as an

investigative procedure that allowed for a "strong, immediate and direct inference" about what was or was not inside the bag: Deschamps J., at paras. 174-75; Bastarache J., at para. 227. Thus, while the "information" obtained by the sniffer dog was simply the smell of the air outside the bag, the dog's reaction to it provided the police with a strong inference as to what was inside. As Binnie J. put it in *A.M.* (which concerned a dog sniff of the accused's backpack), "[b]y use of the dog, the policeman could 'see' through the concealing fabric of the backpack": para. 67.

[29] How to characterize the subject matter of an alleged search was addressed by the Court most recently in *Gomboc*. While the Court was divided on other matters, it was unanimous about the framework that must be applied in considering the subject matter of a "search". The Court considered the strength of the inference between data derived from a digital recording ammeter (DRA) and particular activities going on in a residence in assessing whether use of the DRA constituted a search. Abella J. (Binnie and LeBel JJ. concurring) took into account "the strong and reliable inference that can be made from the patterns of electricity consumption ... as to the presence within the home of one particular activity": para. 81 (emphasis added). The Chief Justice and Justice Fish referred to the fact that the DRA data "sheds light on private activities within the home": para. 119. Deschamps J. (Charron, Rothstein and Cromwell JJ. concurring) spoke in terms of the extent to which the DRA data was revealing of activities in the home: para. 38.

[30] Thus, it is clear that the tendency of information sought to support inferences in relation to other personal information must be taken into account in

characterizing the subject matter of the search. The correct approach was neatly summarized by Doherty J.A. in *Ward*, at para. 65. When identifying the subject matter of an alleged search, the court must not do so "narrowly in terms of the physical acts involved or the physical space invaded, but rather by reference to the nature of the privacy interests potentially compromised by the state action": *ibid.*

[31] Applying this approach to the case at hand, I substantially agree with the conclusion reached by Cameron J.A. in *Trapp* and adopted by Caldwell J.A. in this case. The subject matter of the search was not simply a name and address of someone in a contractual relationship with Shaw. Rather, it was the identity of an Internet subscriber which corresponded to particular Internet usage. As Cameron J.A. put it, at para. 35 of *Trapp*:

> To label information of this kind as mere "subscriber information" or "customer information", or nothing but "name, address, and telephone number information", tends to obscure its true nature. I say this because these characterizations gloss over the significance of an IP address and what such an address, once identified with a particular individual, is capable of revealing about that individual, including the individual's online activity in the home.

[32] Here, the subject matter of the search is the identity of a subscriber whose Internet connection is linked to particular, monitored Internet activity.

(b) *Nature of the Privacy Interest Potentially Compromised by the State Action*

[33] The nature of the privacy interest engaged by the state conduct is another facet of the totality of the circumstances and an important factor in assessing the reasonableness of an expectation of privacy. The Court has previously emphasized an understanding of informational privacy as confidentiality and control of the use of intimate information about oneself. In my view, a somewhat broader understanding of the privacy interest at stake in this case is required to account for the role that anonymity plays in protecting privacy interests online.

[34] Privacy is admittedly a "broad and somewhat evanescent concept": *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403, at para. 67. Scholars have noted the theoretical disarray of the subject and the lack of consensus apparent about its nature and limits: see, e.g., C. D. L. Hunt, "Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for the Development of Canada's Fledgling Privacy Tort" (2011), 37 *Queen's L.J.* 167, at pp. 176-77. Notwithstanding these challenges, the Court has described three broad types of privacy interests — territorial, personal, and informational — which, while often overlapping, have proved helpful in identifying the nature of the privacy interest or interests at stake in particular situations: see, e.g., *Dyment*, at pp. 428-29; *Tessling*, at paras. 21-24. These broad descriptions of types of privacy interests are analytical tools, not strict or mutually-exclusive categories.

[35] The nature of the privacy interest does not depend on whether, in the particular case, privacy shelters legal or illegal activity. The analysis turns on the privacy of the area or the thing being searched and the impact of the search on its

target, not the legal or illegal nature of the items sought. To paraphrase Binnie J. in *Patrick*, the issue is not whether Mr. Spencer had a legitimate privacy interest in concealing his use of the Internet for the purpose of accessing child pornography, but whether people generally have a privacy interest in subscriber information with respect to computers which they use in their home for private purposes: *Patrick*, at para. 32.

[36] We are concerned here primarily with informational privacy. In addition, because the computer identified and in a sense monitored by the police was in Mr. Spencer's residence, there is an element of territorial privacy in issue as well. However, in this context, the location where the activity occurs is secondary to the nature of the activity itself. Internet users do not expect their online anonymity to cease when they access the Internet outside their homes, via smartphones, or portable devices. Therefore, here as in *Patrick*, at para. 45, the fact that a home was involved is not a controlling factor but is nonetheless part of the totality of the circumstances: see, e.g., *Ward*, at para. 90.

[37] To return to informational privacy, it seems to me that privacy in relation to information includes at least three conceptually distinct although overlapping understandings of what privacy is. These are privacy as secrecy, privacy as control and privacy as anonymity.

[38] Informational privacy is often equated with secrecy or confidentiality. For example, a patient has a reasonable expectation that his or her medical information

will be held in trust and confidence by the patient's physician: see, e.g. *McInerney v. MacDonald*, [1992] 2 S.C.R. 138, at p. 149.

[39] Privacy also includes the related but wider notion of control over, access to and use of information, that is, "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others": A. F. Westin, *Privacy and Freedom* (1970), at p. 7, cited in *Tessling*, at para. 23. La Forest J. made this point in *Dyment*. The understanding of informational privacy as control "derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit" (*Dyment*, at p. 429, quoting from *Privacy and Computers*, the Report of the Task Force established by the Department of Communications/Department of Justice (1972), at p. 13). Even though the information will be communicated and cannot be thought of as secret or confidential, "situations abound where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be protected" (pp. 429-30); see also *R. v. Duarte*, [1990] 1 S.C.R. 30, at p. 46.

[40] There is also a third conception of informational privacy that is particularly important in the context of Internet usage. This is the understanding of privacy as anonymity. In my view, the concept of privacy potentially protected by s. 8 must include this understanding of privacy.

[41] The notion of privacy as anonymity is not novel. It appears in a wide array of contexts ranging from anonymous surveys to the protection of police informant identities. A person responding to a survey readily agrees to provide what may well be highly personal information. A police informant provides information about the commission of a crime. The information itself is not private — it is communicated precisely so that it will be communicated to others. But the information is communicated on the basis that it will not be identified with the person providing it. Consider situations in which the police want to obtain the list of names that correspond to the identification numbers on individual survey results or the defence in a criminal case wants to obtain the identity of the informant who has provided information that has been disclosed to the defence. The privacy interest at stake in these examples is not simply the individual's name, but the link between the identified individual and the personal information provided anonymously. As the intervener the Canadian Civil Liberties Association urged in its submissions, "maintaining anonymity can be integral to ensuring privacy": factum, at para. 7.

[42] Westin identifies anonymity as one of the basic states of privacy. Anonymity permits individuals to act in public places but to preserve freedom from identification and surveillance: pp. 31-32; see A. Slane and L. M. Austin, "What's In a Name? Privacy and Citizenship in the Voluntary Disclosure of Subscriber Information in Online Child Exploitation Investigations" (2011), 57 *Crim. L.Q.* 486, at p. 501. The Court's decision in *R. v. Wise*, [1992] 1 S.C.R. 527, provides an example of privacy in a public place. The Court held that the ubiquitous monitoring of a vehicle's whereabouts on public highways amounted to a violation of the

suspect's reasonable expectation of privacy. It could of course have been argued that the electronic device was simply a convenient way of keeping track of where the suspect was driving his car, something that he was doing in public for all to see. But the Court did not take that approach.

[43] La Forest J. (who, while dissenting on the issue of exclusion of the evidence under s. 24(2), concurred with respect to the existence of a reasonable expectation of privacy), explained that "[i]n a variety of public contexts, we may expect to be casually observed, but may justifiably be outraged by intensive scrutiny. In these public acts we do not expect to be personally identified and subject to extensive surveillance, but seek to merge into the 'situational landscape'": p. 558 (emphasis added), quoting M. Gutterman, "A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance" (1988), 39 *Syracuse L. Rev.* 647, at p. 706. The mere fact that someone leaves the privacy of their home and enters a public space does not mean that the person abandons all of his or her privacy rights, despite the fact that as a practical matter, such a person may not be able to control who observes him or her in public. Thus, in order to uphold the protection of privacy rights in some contexts, we must recognize anonymity as one conception of privacy: see E. Paton-Simpson, "Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places" (2000), 50 *U.T.L.J.* 305, at pp. 325-26; Westin, at p. 32; Gutterman, at p. 706.

[44] Recognizing that anonymity is one conception of informational privacy seems to me to be particularly important in the context of Internet usage. One form of

anonymity, as Westin explained, is what is claimed by an individual who wants to present ideas publicly but does not want to be identified as their author: p. 32. Here, Westin, publishing in 1970, anticipates precisely one of the defining characteristics of some types of Internet communication. The communication may be accessible to millions of people but it is not identified with its author.

[45] Moreover, the Internet has exponentially increased both the quality and quantity of information that is stored about Internet users. Browsing logs, for example, may provide detailed information about users' interests. Search engines may gather records of users' search terms. Advertisers may track their users across networks of websites, gathering an overview of their interests and concerns. "Cookies" may be used to track consumer habits and may provide information about the options selected within a website, which web pages were visited before and after the visit to the host website and any other personal information provided: see N. Gleicher, "Neither a Customer Nor a Subscriber Be: Regulating the Release of User Information on the World Wide Web" (2009), 118 *Yale L.J.* 1945, at pp. 194849; R. W. Hubbard, P. DeFreitas and S. Magotiaux, "The Internet — Expectations of Privacy in a New Context" (2002), 45 *Crim. L.Q.* 170, at pp. 189-91. The user cannot fully control or even necessarily be aware of who may observe a pattern of online activity, but by remaining anonymous — by guarding the link between the information and the identity of the person to whom it relates — the user can in large measure be assured that the activity remains private: see Slane and Austin, at pp. 500-3.

[46] In my view, the identity of a person linked to their use of the Internet must be recognized as giving rise to a privacy interest beyond that inherent in the person's name, address and telephone number found in the subscriber information. A sniffer dog provides information about the contents of the bag and therefore engages the privacy interests relating to its contents. DRA readings provide information about what is going on inside a home and therefore may engage the privacy interests relating to those activities. Similarly, subscriber information, by tending to link particular kinds of information to identifiable individuals, may implicate privacy interests relating not simply to the person's name or address but to his or her identity as the source, possessor or user of that information.

[47] Doherty J.A. made this point with his usual insight and clarity in *Ward*. "Personal privacy" he wrote "protects an individual's ability to function on a day-to-day basis within society while enjoying a degree of anonymity that is essential to the individual's personal growth and the flourishing of an open and democratic society": para. 71. He concluded that some degree of anonymity is a feature of much Internet activity and that, "depending on the totality of the circumstances, . . . anonymity may enjoy constitutional protection under s. 8": para. 75. I agree. Thus, anonymity may, depending on the totality of the circumstances, be the foundation of a privacy interest that engages constitutional protection against unreasonable search and seizure.

[48] The intervener the Director of Public Prosecutions raised the concern that recognizing a right to online anonymity would carve out a crime-friendly Internet landscape by impeding the effective investigation and prosecution of online crime. In

light of the grave nature of the criminal wrongs that can be committed online, this concern cannot be taken lightly. However, in my view, recognizing that there *may* be a privacy interest in anonymity depending on the circumstances falls short of recognizing any "right" to anonymity and does not threaten the effectiveness of law enforcement in relation to offences committed on the Internet. In this case, for example, it seems clear that the police had ample information to obtain a production order requiring Shaw to release the subscriber information corresponding to the IP address they had obtained.

[49] Applying this framework to the facts of the present case is straightforward. In the circumstances of this case, the police request to link a given IP address to subscriber information was in effect a request to link a specific person (or a limited number of persons in the case of shared Internet services) to specific online activities. This sort of request engages the anonymity aspect of the informational privacy interest by attempting to link the suspect with anonymously undertaken online activities, activities which have been recognized by the Court in other circumstances as engaging significant privacy interests: *R. v. Morelli*, 2010 SCC 8, [2010] 1 S.C.R. 253, at para. 3; *Cole*, at para. 47; *R. v. Vu*, 2013 SCC 60, [2013] 3 S.C.R. 657, at paras. 40-45.

[50] I conclude therefore that the police request to Shaw for subscriber information corresponding to specifically observed, anonymous Internet activity engages a high level of informational privacy. I agree with Caldwell J.A.'s conclusion on this point:

> [A] reasonable and informed person concerned about the protection of privacy would expect one's activities on one's own computer used in one's own home would be private . . . In my judgment, it matters not that the personal attributes of the Disclosed Information pertained to Mr. Spencer's sister because Mr. Spencer was personally and directly exposed to the consequences of the police conduct in this case. As such, the police conduct *prima facie* engaged a personal privacy right of Mr. Spencer and, in this respect, his interest in the privacy of the Disclosed Information was direct and personal. [para. 27]

(c) *Reasonable Expectation of Privacy*

[51] The next question is whether Mr. Spencer's expectation of privacy was reasonable. The trial judge found that there could be no reasonable expectation of privacy in the face of the relevant contractual and statutory provisions (para. 19), a conclusion with which Caldwell J.A. agreed on appeal: para. 42. Cameron J.A., however, was doubtful that the contractual and statutory terms had this effect in the context of this case: para. 98.

[52] In this Court, Mr. Spencer maintains that the contractual and statutory terms did not undermine a reasonable expectation of privacy with respect to the subscriber information. He submits that the contractual provisions do nothing more than suggest that the information will not be provided to police unless required by law and that *PIPEDA*, whose purpose is to protect privacy rights, supports rather than negates the reasonableness of an expectation of privacy in this case. The Crown disagrees and supports the position taken on this point by Caldwell J.A. in the Court of Appeal.

[53] There is no doubt that the contractual and statutory framework may be relevant to, but not necessarily determinative of whether there is a reasonable expectation of privacy. So, for example in *Gomboc*, Deschamps J. writing for four members of the Court, found that the terms governing the relationship between the electricity provider and its customer were "highly significant" to Mr Gomboc's reasonable expectation of privacy, but treated it as "one factor amongst many others which must be weighed in assessing the totality of the circumstances": paras. 31-32. She also emphasized that when dealing with contracts of adhesion in the context of a consumer relationship, it was necessary to "procee[d] with caution" when determining the impact that such provision would have on the reasonableness of an expectation of privacy: para. 33. The need for caution in this context was pointedly underlined in the dissenting reasons of the Chief Justice and Fish J. in that case: paras. 138-42.

[54] The contractual and regulatory frameworks overlap in the present case because the Shaw Joint Terms of Service make reference to *PIPEDA*, and the scope of permitted disclosure under *PIPEDA* turns partly on whether the customer has consented to the disclosure of personal information. I must first set out the details of these schemes before turning to their impact on the reasonable expectations analysis. In doing so, it becomes apparent that the relevant provisions provide little assistance in evaluating the reasonableness of Mr. Spencer's expectation of privacy.

[55] Shaw provides Internet services to its customers under a standard form "Joint Terms of Service" agreement. Additional terms and conditions are provided in

Shaw's "Acceptable Use Policy" and its "Privacy Policy". The terms of these agreements are posted online on Shaw's website and change from time to time. The investigators sought the subscriber information for the IP address used on August 31, 2007 in their request to Shaw.

[56] Mr. Spencer was not personally a party to these agreements, as he accessed the Internet through his sister's subscription. It is common practice for multiple users to share a common Internet connection. A reasonable user would be aware that the use of the service would be governed by certain terms and conditions, and those terms and conditions were readily accessible through Shaw's website. This case does not require us to decide whether Mr. Spencer was bound by the terms of the contract with Shaw. Quite apart from contractual liability, the terms on which he gained access to the Internet are a relevant circumstance in assessing the reasonableness of his expectation of privacy. There are three relevant sets of provisions which, taken as a whole, provide a confusing and unclear picture of what Shaw would do when faced with a police request for subscriber information. The "Joint Terms of Service" at first blush appear to permit broad disclosure because they provide, among other things, that "Shaw may disclose any information as is necessary to . . . satisfy any legal, regulatory or other governmental request". This general provision, however, must be read in light of the more specific provision relating to disclosure of IP addresses and other identifying information in the context of criminal investigations contained in the Acceptable Use Policy, which in turn is subject to the Privacy Policy.

[57] The Acceptable Use Policy (last updated on June 18, 2007) provides that Shaw is authorized to cooperate with law enforcement authorities in the investigation of criminal violations, including supplying information identifying a subscriber *in accordance with its Privacy Policy*. The provision reads as follows:

> You hereby authorize Shaw to cooperate with (i) law enforcement authorities in the investigation of suspected criminal violations, and/or (ii) system administrators at other Internet service providers or other network or computing facilities in order to enforce this Agreement. Such cooperation may include Shaw providing the username, IP address or other identifying information about a subscriber, in accordance with the guidelines set out in Shaw's Privacy Policy. [Emphasis added.]

[58] The Privacy Policy in the record (last updated on November 12, 2008) states that Shaw is committed to protecting personal information, which is defined as information about an identifiable individual. One of the ten principles set out in the Privacy Policy deals with limiting the disclosure of personal information (principle 5). The policy limits the circumstances under which personal information will be disclosed without the customer's knowledge or consent to "exceptional circumstances, as permitted by law". Shaw may disclose information to its partners in order to provide its services and, in such cases, the information is governed by "strict confidentiality standards and policies" to keep the information secure and to ensure it is treated in accordance with *PIPEDA*. The Privacy Policy also provides that "Shaw may disclose Customer's Personal Information to: . . . a third party or parties, where the Customer has given Shaw Consent to such disclosure or if disclosure is required by law, in accordance with *The Personal Information Protection and Electronic Documents Act*" (emphasis added).

[59] Whether or not disclosure of personal information by Shaw is "permitted" or "required by law" in turn depends on an analysis of the applicable statutory framework. The contractual provisions, read as a whole, are confusing and equivocal in terms of their impact on a user's reasonable expectation of privacy in relation to police initiated requests for subscriber information. The statutory framework provided by *PIPEDA* is not much more illuminating.

[60] Shaw's collection, use, and disclosure of the personal information of its subscribers is subject to *PIPEDA* which protects personal information held by organizations engaged in commercial activities from being disclosed without the knowledge or consent of the person to whom the information relates: Sch. 1, clause 4.3. Section 7 contains several exceptions to this general rule and permits organizations to disclose personal information without consent. The exception relied on in this case is s. 7(3)(*c.1*)(ii). It permits disclosure to a government institution that has requested the disclosure for the purpose of law enforcement and has stated its "lawful authority" for the request. The provisions of *PIPEDA* are not of much help in determining whether there is a reasonable expectation of privacy in this case. They lead us in a circle.

[61] Section 7(3)(*c.1*)(ii) allows for disclosure without consent to a government institution where that institution has identified its *lawful authority* to obtain the information. But the issue is whether there was such lawful authority which in turn depends in part on whether there was a reasonable expectation of privacy with respect to the subscriber information. *PIPEDA* thus cannot be used as a factor to

weigh against the existence of a reasonable expectation of privacy since the proper interpretation of the relevant provision itself depends on whether such a reasonable expectation of privacy exists. Given that the purpose of *PIPEDA* is to establish rules governing, among other things, disclosure "of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information" (s. 3), it would be reasonable for an Internet user to expect that a simple request by police would not trigger an obligation to disclose personal information or defeat *PIPEDA*'s general prohibition on the disclosure of personal information without consent.

[62] I am aware that I have reached a different result from that reached in similar circumstances by the Ontario Court of Appeal in *Ward*, where the court held that the provisions of *PIPEDA* were a factor which weighed against finding a reasonable expectation of privacy in subscriber information. This conclusion was based on two main considerations. The first was that an ISP has a legitimate interest in assisting in law enforcement relating to crimes committed using its services: para. 99. The second was the grave nature of child pornography offences, which made it reasonable to expect that an ISP would cooperate with a police investigation: paras. 102-3. While these considerations are certainly relevant from a policy perspective, they cannot override the clear statutory language of s. 7(3)(*c.1*)(ii) of *PIPEDA*, which permits disclosure only if a request is made by a government institution with "lawful authority" to request the disclosure. It is reasonable to expect that an organization bound by *PIPEDA* will respect its statutory obligations with respect to personal information. The Court of Appeal in *Ward* held that s. 7(3)(*c.1*)(ii)

must be read in light of s. 5(3), which states that "[a]n organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances". This rule of "reasonable disclosure" was used as a basis to invoke considerations such as allowing ISPs to cooperate with the police and preventing serious crimes in the interpretation of *PIPEDA*. Section 5(3) is a guiding principle that underpins the interpretation of the various provisions of *PIPEDA*. It does not allow for a departure from the clear requirement that a requesting government institution possess "lawful authority" and so does not resolve the essential circularity of using s. 7(3)(*c.1*)(ii) as a factor in determining whether a reasonable expectation of privacy exists.

[63] I also note with respect to an ISP's legitimate interest in preventing crimes committed through its services that entirely different considerations may apply where an ISP itself detects illegal activity and of its own motion wishes to report this activity to the police. Such a situation falls under a separate, broader exemption in *PIPEDA*, namely s. 7(3)(*d*). The investigation in this case was begun as a police investigation and the disclosure of the subscriber information arose out of the request letter sent by the police to Shaw.

[64] The overall impression created by these terms is that disclosure at the request of the police would be made only where required or permitted by law. Such disclosure is only permitted by *PIPEDA* in accordance with the exception in s. 7, which in this case would require the requesting police to have "lawful authority" to request the disclosure. For reasons that I will set out in the next section, this request

had no lawful authority in the sense that while the police could ask, they had no authority to compel compliance with that request. I conclude that, if anything, the contractual provisions in this case support the existence of a reasonable expectation of privacy, since the Privacy Policy narrowly circumscribes Shaw's right to disclose the personal information of subscribers.

[65] In my view, in the totality of the circumstances of this case, there is a reasonable expectation of privacy in the subscriber information. The disclosure of this information will often amount to the identification of a user with intimate or sensitive activities being carried out online, usually on the understanding that these activities would be anonymous. A request by a police officer that an ISP voluntarily disclose such information amounts to a search.

[66] The intervener the Attorney General of Alberta raised a concern that if the police were not permitted to request disclosure of subscriber information, then other routine inquiries that might reveal sensitive information about a suspect would also be prohibited, and this would unduly impede the investigation of crimes. For example, when the police interview the victim of a crime, core biographical details of a suspect's lifestyle might be revealed. I do not agree that this result follows from the principles set out in these reasons. Where a police officer requests disclosure of information relating to a suspect from a third party, whether there is a search depends on whether, in light of the totality of the circumstances, the suspect has a reasonable expectation of privacy in that information: *Plant*, at p. 293; *Gomboc*, at paras. 27-30, *per* Deschamps J. In *Duarte*, the Court distinguished between a person repeating a

conversation with a suspect to the police and the police procuring an audio recording of the same conversation. The Court held that the danger is "not the risk that someone will repeat our words but the much more insidious danger inherent in allowing the state, in its unfettered discretion, to record and transmit our words": at pp. 43-44. Similarly in this case, the police request that the ISP disclose the subscriber information was in effect a request to link Mr. Spencer with precise online activity that had been the subject of monitoring by the police and thus engaged a more significant privacy interest than a simple question posed by the police in the course of an investigation.