

Court File Numbers:  
C50206 & C52091

**COURT OF APPEAL FOR ONTARIO**

**B E T W E E N:**

**DAVID WARD and DOUGLAS CUTTELL**

**APPELLANTS**

**- and -**

**HER MAJESTY THE QUEEN**

**RESPONDENT**

**- and -**

**THE CANADIAN CIVIL LIBERTIES ASSOCIATION**

**INTERVENER**

---

**FACTUM OF THE INTERVENER  
THE CANADIAN CIVIL LIBERTIES ASSOCIATION**

---

**JAMES STRIBOPOULOS**  
KAPOOR BARRISTERS  
20 Adelaide St. E.  
Suite # 210  
Toronto, Ontario  
M5C 2T6

Tel: 416-363-2700  
Fax: 416-368-6811  
Email: [jst@kapoorbarristers.com](mailto:jst@kapoorbarristers.com)

**COUNSEL FOR THE INTERVENER**

**GRAEME NORTON**  
CANADIAN CIVIL LIBERTIES ASSOCIATION  
360 Bloor Street West  
Suite # 506  
Toronto, Ontario  
M5S 1X1

Tel: 416-363-3021  
Fax: 416-861-1291  
Email: [gnorton@ccla.org](mailto:gnorton@ccla.org)

**COUNSEL FOR THE INTERVENER**

**JONATHAN DAWE**  
SACK GOLDBLATT MITCHELL LLP  
20 Dundas Street West  
Suite #1100  
Toronto, Ontario  
M5G 2G8

Tel: 416-979-6447  
Fax: 416-591-7333  
email: [jdawe@sgmlaw.com](mailto:jdawe@sgmlaw.com)

COUNSEL FOR THE APPELLANT WARD

**JILL R. PRESSER**  
SCHRECK PRESSER LLP  
6 Adelaide Street East  
5th Floor  
Toronto, Ontario  
M5C 2H6

Tel: 416.586.0330  
Fax: 416.977.8513  
email: [presser@schreckpresser.com](mailto:presser@schreckpresser.com)

COUNSEL FOR THE APPELLANT CUTTELL

**MICHAL FAIRBURN**  
MINISTRY OF THE ATTORNEY  
GENERAL FOR ONTARIO  
Crown Law Office – Criminal  
720 Bay Street, 10<sup>th</sup> Floor  
Toronto, Ontario  
M5G 2K1

Tel: 416-326-2002  
Fax: 416-326-4656  
email: [michal.fairburn@ontario.ca](mailto:michal.fairburn@ontario.ca)

COUNSEL FOR THE RESPONDENT

## TABLE OF CONTENTS

	<b>PAGE</b>
PART I – STATEMENT OF THE CASE .....	1
PART II – STATEMENT OF THE FACTS .....	3
PART III - ISSUES AND THE LAW .....	3
A. Overview of the <i>CCLA</i> 's Position .....	3
B. Piercing the Anonymity of an IP Address Encroaches Upon a Reasonable Expectation of Privacy .....	5
C. Subsection 7(3)(c.1) of <i>PIPEDA</i> Does Not Create a Police Power to Pierce the Anonymity of IP Addresses.....	13
D. Consumer Agreements that Track the Language of the <i>PIPEDA</i> Exceptions Should Play No Role In Defining Canadians' Reasonable Privacy Expectations .....	17
PART IV – ORDER REQUESTED .....	20
SCHEDULE A – TABLE OF AUTHORITIES .....	21
SCHEDULE B – RELEVANT LEGISLATIVE PROVISIONS .....	24

**COURT OF APPEAL FOR ONTARIO**

**B E T W E E N:**

**DAVID WARD and DOUGLAS CUTTELL**

**APPELLANTS**

**- and -**

**HER MAJESTY THE QUEEN**

**RESPONDENT**

**- and -**

**THE CANADIAN CIVIL LIBERTIES ASSOCIATION**

**INTERVENER**

---

**FACTUM OF THE INTERVENER  
THE CANADIAN CIVIL LIBERTIES ASSOCIATION**

---

**PART I – STATEMENT OF THE CASE**

1. At issue in these appeals is the reasonable expectation of privacy enjoyed by Canadians when using the Internet. Specifically, whether s. 8 of the *Charter* requires that police obtain a warrant before piercing the anonymity of an Internet Protocol address (“IP address”) and gaining access to the identity of an Internet user. Revealing such information is the key to connecting an individual to their online activities. Accordingly, whether or not a warrant is required to access an Internet user’s IP address will ultimately determine the extent to which Canadians will enjoy privacy when browsing and surfing the Internet.

2. In each of the cases under appeal, the Appellants were convicted of a variety of child pornography related offences. At trial, each challenged the admissibility of evidence obtained by police following the execution of search warrants. The basis of these challenges was essentially the same. In both cases, the constitutional complaint was directed at the accessing of information by police that served to reveal the identity and address of a computer user (“subscriber information”) behind a particular IP that had visited websites featuring child pornography and viewed, downloaded and, in the case of *Cuttell*, shared, such images. In both cases, this subscriber information was acquired without a warrant and then used to obtain warrants that were ultimately executed and yielded evidence of child pornography related offences. In each case, the accused argued at trial that when the unconstitutionally acquired information was excised from the Information to Obtain, what remained was fatally deficient, that the searches and seizures undertaken violated their s. 8 *Charter* rights and that the evidence obtained should be excluded under s. 24(2).

3. In the two cases on appeal the lower courts arrived at differing conclusions as to whether the accessing of subscriber information encroaches upon a reasonable expectation of privacy so as to engage s. 8 of the *Charter*. (There has also been a lack of consensus amongst other courts that have considered the issue.<sup>1</sup>) In *Ward*, Lalande J. found no

---

<sup>1</sup> Some courts have found that gaining access to subscriber information encroaches upon a reasonable expectation of privacy and engages s. 8 of the *Charter*. See *R. v. Kwok*, [2008] O.J. No. 2414 (C.J.); *Re C.(S.)*, [2006] O.J. No. 3754 (C.J.). But other courts have come to the opposite conclusion. See *R. v. Friers*, [2008] O.J. No. 5646 (C.J.); *R. v. Wilson*, [2009] O.J. No. 1067 (S.C.J.); *R. v. Vasic* (2009), 185 C.R.R. (2d) 286 (Ont. S.C.J.); *R. v. McGarvie*, 2009 CarswellOnt 500 (C.J.); *R. v. Verge*, 2009 CarswellOnt 501 (C.J.); *R. v. Brousseau* (2010), 264 C.C.C. (3d) 562 (Ont.S.C.J.). The question has also been considered by the courts in other provinces, which have rejected the existence of a reasonable expectation of privacy. See *R. v. Spencer* (2009), 361 Sask.R. 1 (Q.B.); *R. v. Trapp* (2009), 330 Sask. R. 169 (Prov. Ct.); *R. v. McNeice*, [2010] B.C.J. No. 2131 (S.C.). No Canadian appellate court has yet addressed the

reasonable expectation of privacy in subscriber information and therefore found no s. 8 *Charter* violation.<sup>2</sup> By contrast, in *Cuttell*, Pringle J. found a reasonable expectation of privacy in such information and held that Mr. Cuttell's s. 8 *Charter* rights were therefore violated when police gained access to his subscriber information without a warrant. In the result, however, she ruled the evidence obtained admissible under s. 24(2).<sup>3</sup>

4. Accordingly, the Appellants were both convicted and each appeals their convictions to this Honourable Court. These appeals therefore raise a fundamentally important question regarding the extent to which Canadians will enjoy privacy in their online activities when surfing and browsing the Internet.

## **PART II – STATEMENT OF THE FACTS**

5. The Intervener, the *Canadian Civil Liberties Association* (“CCLA”) accepts as correct the Statement of Facts contained in the respective Appellants’ Factums.

## **PART III – ISSUES AND LAW**

### **A. Overview of the CCLA’s Position**

6. It is the position of the *CCLA* that Canadians enjoy a reasonable expectation of privacy that is deserving of protection under s. 8 of the *Charter* with respect to their browsing and surfing activities when using the Internet. An individual’s activities on the Internet can reveal highly personal and intimate information about them, providing considerable insight into the user’s interests, habits, predilections and, by implication, their

---

question. Although the Saskatchewan Court of Appeal heard argument on appeal in *Trapp, supra*, in November 2010, as of May 2011, judgment remains on reserve in that case.

<sup>2</sup> See *R. v. Ward* (2008), 176 C.R.R. (2d) 90 (Ont.C.J.).

<sup>3</sup> See *R. v. Cuttell* (2009), 247 C.C.C. (3d) 424 (Ont.C.J.).

very thoughts. Because piercing the anonymity supplied by an IP address is the key to gaining access to a vast repository of highly personal information regarding an individual's online activities, s. 8 of the *Charter* is engaged by such an intrusion. Consequently, in order for the police to gain access to the subscriber information behind an IP address, absent exigent circumstances, they are constitutionally required to subject their supporting grounds to prior judicial scrutiny through the warrant process. (See ¶ 9 to ¶ 22 below.)

7. The *CCLA* submits that provisions found in the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 (“*PIPEDA*”), the purpose of which is to *protect* the privacy of Canadians (*Ibid.* s. 3), should not be construed so as to license warrantless access to the subscriber information behind IP addresses. To the extent that lower courts have construed subsection 7(3)(c.1) of *PIPEDA* in this way, including the court below in *Ward*, the *CCLA* submits that this interpretation is in error. Properly construed, in light of its plain wording, the larger purposes of *PIPEDA*, and *Charter* values, that provision simply creates an exception to the general obligation on “organizations” to keep “personal information” they acquire confidential (*Ibid.* s. 5(1)). Subsection 7(3)(c.1) enables an organization to comply with law enforcement requests, *provided* the request is premised on “lawful authority”. In short, this provision does *not* create a *new* police search and seizure power. Rather, it merely facilitates the execution of *existing powers*. In the criminal investigative realm, the established lawful authority by which police may intrude upon a reasonable expectation of privacy, in the absence of exigent circumstances, is a warrant. (See ¶ 23 to ¶ 28 below.)

8. Finally, although the terms of agreements between subscribers and Internet Service Providers have figured prominently when the issues raised by these appeals have been

litigated in the courts below, as happened in *Ward*, the *CCLA* submits that the terms of such agreements should not be decisive of the scope of the individual's reasonable privacy expectations. First, it must be remembered that the terms of these agreements have essentially been directed by *PIPEDA*. Contractual terms mandated by legislation should not define the parameters of reasonable privacy expectations under s. 8 of the *Charter*. It would also be dangerous to allow Canadians' reasonable privacy expectations to be defined by the fine print found in the contracts of adhesion that pervade modern commercial relationships. Ultimately, the scope of Canadians' reasonable expectations of privacy is a normative question that cannot be directed or determined by the fine print of rarely read or understood contractual terms. (See ¶ 29 to ¶ 33 below.)

### **B. Piercing the Anonymity of an IP Address Encroaches Upon A Reasonable Expectation of Privacy**

9. The Supreme Court of Canada has repeatedly cautioned against the use of *ex post facto* reasoning in evaluating constitutional claims under s. 8 of the *Charter*,<sup>4</sup> explaining that the purpose of the guarantee “is to *prevent* unreasonable intrusions on privacy, not to sort them out from reasonable intrusions on an *ex post facto* analysis”.<sup>5</sup> According to the Court, this approach is “inherent in the notion of being secure against unreasonable searches and seizures”.<sup>6</sup> As a result, the Court has directed that decisions as to whether or not s. 8 is engaged must be made from an *ex ante* perspective, without regard to the fact

---

<sup>4</sup> See *Hunter v. Southam Inc.*, (1984), 14 C.C.C. (3d) 97 at 109 (S.C.C.); *R. v. Wong* (1990) 60 C.C.C. (3d) 460 at 480-81 (S.C.C.); *R. v. Greffe*, (1990) 55 C.C.C. (3d) 161 at 176, 187-88 (S.C.C.) *R. v. Dymont* (1988) 45 C.C.C. (3d) 244 at 256 (S.C.C.); *R. v. Kokesch* (1990) 61 C.C.C. (3d) 207 at 227 (S.C.C.); *R. v. Feeney* (1997), 115 C.C.C. (3d) 129 at 154-55, 157, 159 (S.C.C.); *R. v. Buhay* (2003), 174 C.C.C. (3d) 97 at para. 19 (S.C.C.); *R. v. A.M.* (2008), 230 C.C.C. (3d) 377 at paras. 5, 70 (S.C.C.).

<sup>5</sup> *Feeney*, *supra*, at 155.

<sup>6</sup> *Dymont*, *supra*, at 256.

that evidence of illegal activity was discovered. Instead, in evaluating claims under s. 8 of the *Charter*, “the question must be framed in broad and neutral terms”<sup>7</sup>. This approach requires a reviewing court to ask what law-abiding Canadians would reasonably expect in the circumstances.<sup>8</sup>

10. Framed in broad and neutral terms, the question presented by the cases on appeal is whether, in a society such as ours, persons have a reasonable expectation of privacy in information that would reveal their association with an IP address and serve to disclose their online activities when browsing and surfing the Internet?

11. In answering that question, the Supreme Court has instructed that the “totality of the circumstances” must be considered.<sup>9</sup> In that regard, the Court has placed particular emphasis on two principal considerations, whether the accused had a subjective expectation of privacy and whether that expectation of privacy was objectively reasonable.<sup>10</sup> Within that general framework, because “privacy is a varied and wide-ranging concept,”<sup>11</sup> the Supreme Court has also recognized that privacy manifests itself in a number of different and sometimes overlapping contexts, including personal privacy, territorial privacy and informational privacy.<sup>12</sup> Most important for the two cases on appeal

---

<sup>7</sup> *Wong, supra*, at 481. See also *Buhay, supra*, para. 19.

<sup>8</sup> *Ibid.*

<sup>9</sup> *R. v. Edwards* (1996), 104 C.C.C. (3d) 136 at para. 45 (S.C.C.). See also *Buhay, supra* at paras. 18-19.

<sup>10</sup> See *R. v. Tessling* (2004), 189 C.C.C. (3d) 189 at para. 19 (S.C.C.); *R. v. Kang-Brown* (2008), 230 C.C.C. (3d) 289 at para. 140 (S.C.C.); *R. v. Patrick* (2009), 242 C.C.C. (3d) 158 at para. 26 (S.C.C.); *R. v. Gomboc*, [2010] 3 S.C.R. 211 at para. 18.

<sup>11</sup> *Gomboc, supra*, at para. 19.

<sup>12</sup> *Ibid.* See also *Tessling, supra* at paras. 20-24 (S.C.C.); *Dyment, supra* at 255.

is the Supreme Court's jurisprudence sketching out the general parameters of Canadians' reasonable privacy expectations in the context of informational privacy claims.

12. The Supreme Court has repeatedly affirmed the importance of informational privacy and its protection under s. 8 of the *Charter*. As LaForest J. noted in *Dyment*:

In modern society, especially, retention of information about oneself is extremely important. We may, for one reason or another, wish or be compelled to reveal such information, but situations abound where the reasonable expectations of the individual that information shall remain confidential to the persons to whom, and restricted to the purpose for which it is divulged, must be protected.<sup>13</sup>

13. In *Plant*, a 1993 decision that preceded the rise of the Internet, the Supreme Court identified a number of specific factors to be taken into account in deciding whether an individual will enjoy a reasonable expectation of privacy in information. The Court explained that,

... the nature of the information itself, the nature of the relationship between the party releasing the information and the party claiming its confidentiality, the place where the information was obtained, the manner in which it was obtained and the seriousness of the crime being investigated allow for a balancing of the societal interests in protecting individual dignity, integrity and autonomy with effective law enforcement.<sup>14</sup>

14. In *Plant*, the Court refrained from following the lead of the United States Supreme Court, which has refused to extend the Fourth Amendment's protections to commercial information. Instead, the Court made clear that commercial records in the possession of third parties may be subject to a reasonable expectation of privacy under s. 8 of the *Charter*, if the relevant information bears upon:

---

<sup>13</sup> *Dyment*, *supra* at 255-56. See also *Tessling*, *supra* at para. 23.

<sup>14</sup> *R. v. Plant* (1993) 84 C.C.C. (3d) 204 at 212 (S.C.C.). See also *R. v. Dersch* (1993), 85 C.C.C. (3d) 1 at 13 (S.C.C.). However, In *Tessling* the Court indicated that the "seriousness of the crime" should no longer be considered at the threshold level when determining whether section 8 of the *Charter* is engaged. Rather, the Court explained that that factor should be left for consideration when deciding on the reasonableness of the intrusion or the appropriate remedy under section 24(2) of the *Charter*. See *Tessling*, *supra* at para. 64

... a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual.<sup>15</sup>

15. The Supreme Court has applied the factors identified in *Plant* in a number of cases. In *Plant* itself, the electrical consumption records at issue were held not to qualify, partly because they revealed very little about the personal lifestyle or private decisions of the residents and also due to the fact that they were otherwise publicly available. More recently, in *Gomboc* the Court was sharply divided as to whether s. 8 was engaged where the police employed a digital recording ammeter to measure the moment-by-moment flow of electricity entering a home.<sup>16</sup> The Court has, however, recognized a reasonable expectation of privacy in information supplied by a patient to medical personnel.<sup>17</sup> It came to the same conclusion with respect to information shared by a complainant with a therapist.<sup>18</sup> It also concluded that the victim of a theft retained a reasonable expectation of privacy in financial records located in a stolen safe.<sup>19</sup> In addition, some members of the

---

<sup>15</sup> *Plant, supra* 213.

<sup>16</sup> *Gomboc, supra*. McLachlin C.J. and Fish J., dissenting, concluded it was. Binnie, LeBel and Abella JJ. also suggested that, in theory, it would be. In concluding that s. 8 was not engaged on the facts of this case, they noted that a provincial regulation entitled the customer to request confidentiality in information regarding his electrical consumption but emphasized that the Respondent had not done so. In contrast, Deschamps, Charron, Rothstein and Cromwell JJ. concluded that the information that a digital recording ammeter could reveal about the consumption of electricity in the home was not sufficiently personal and intimate to qualify for protection under s. 8.

<sup>17</sup> *Dersch, supra*.

<sup>18</sup> *R. v. Mills* (1999), 139 C.C.C. (3d) 321 (S.C.C.).

<sup>19</sup> *R. v. Law* (2002), 160 C.C.C. (3d) 449 (S.C.C.).

Court have indicated that, in their view, individuals enjoy a reasonable expectation of privacy in their personal banking records.<sup>20</sup>

16. Although the Supreme Court has not yet directly addressed Canadians' privacy expectations in the context of the Internet, its recent decision in *Morelli* brings into focus the privacy concern at the heart of these appeals. In *Morelli*, in the course of remarking on the profound intrusiveness of computer searches, Fish J., for the majority, emphasized that one of the reasons such searches are so invasive is because they permit: "[t]he police [to] scrutinize as well the electronic roadmap of your cybernetic peregrinations, where you have been and what you appear to have seen on the Internet — generally by design, but sometimes by accident."<sup>21</sup>

17. The concern expressed in the excerpt from *Morelli* is precisely what is at stake in these appeals. However, rather than determining where an individual has been on the Internet from scouring their computer hard drive, piercing the anonymity provided by an IP address will permit the police to glean similarly revealing information about an Internet user without taking physical control of a computer. To understand this, one requires a sense of how the Internet functions. Online an individual enjoys anonymity (and therefore privacy) through the protection afforded by an Internet Protocol (IP) address (consisting of a series of numbers of varying length). Although an individual's online activities leave an

---

<sup>20</sup> *Schreiber v. Canada (A.G.)*, (1998), 124 C.C.C. (3d) 129 at paras. 22, 55 (S.C.C.) the Court considered whether the seizure of a suspect's foreign banking records engaged s. 8 of the *Charter*. The majority concluded that the Canadian government's request for foreign assistance did not engage s. 8; it declined to consider whether a warrantless search of a suspect's domestic banking records would have attracted a reasonable expectation of privacy. In his concurring reasons, Lamer C.J. indicated that he would have answered "yes" to this question. *Ibid.* at para. 22. In his dissent, Iacobucci J. concluded that the suspect did have a reasonable expectation of privacy in his foreign banking records. *Ibid.* at para. 55.

<sup>21</sup> *R. v. Morelli*, [2010] 1 S.C.R. 253 at para. 3.

electronic trail wherever the user travels on the Internet, in the form of their IP address, *only* the user (if they are tech savvy) and their Internet Service Provider (ISP) know the identity behind a particular IP address. In other words, the user's identity is shielded from public view through the IP address. This information is *not* in the public domain.

18. Piercing the anonymity provided by an Internet user's IP address does not simply reveal that user's name and residential address, as some lower courts that have rejected the existence of a reasonable expectation of privacy have held (including the court below in *Ward*).<sup>22</sup> Construing what is at stake in this narrow way would serve to completely de-contextualize the larger informational privacy interests that are directly implicated by these appeals. The Supreme Court has emphasized that when it comes to determining whether a reasonable expectation of privacy is implicated, "[t]he assessment *always* requires close attention to context."<sup>23</sup> One's name, depending on the context, can be the key to unlocking a wealth of personal information that an individual would reasonably expect to remain confidential.<sup>24</sup> Associating an Internet user's name with a particular IP address can expose both her identity *and the content of her on-line activities*. This is significantly more privacy invasive than linking a person to a particular phone number or municipal address.

---

<sup>22</sup> See *Ward, supra* at para. 67; *Wilson, supra* at para. 42; *Frier, supra* at para. 24.

<sup>23</sup> *Patrick, supra*, at para. 26 (italics added). See also *Gomboc, supra*: "I reiterate before undertaking that analysis that context is crucial and that reasonable expectation of privacy is assessed in the totality of the circumstances." *Ibid* at para. 23.

<sup>24</sup> See *R. v. Eddy* (1994) 119 Nfld. & PEIR 91 (Nfld. S.C.T.D.), making this point in the context of banking records, explaining that: "The linkage of a name to [account] information creates at once the intimate relationship between that information and the particular individual, which is the essence of the privacy interest. I do not accept the Crown's suggestion that the mere obtaining of the name of the owner of an account about which information is already available is not deserving of protection under s.8." *Ibid.* at para. 175.

19. This Court has previously recognized that gaining access to an individual's name may have significant privacy implications. In *Harris*<sup>25</sup> this Court held that police violated s. 8 of the *Charter* when they asked a motor vehicle passenger his name during a traffic stop. The reason for the request was to undertake a police background check in order to determine if the passenger had any outstanding warrants or was breaching probation or bail conditions. In rejecting the Crown's argument that one can never enjoy a reasonable expectation of privacy in their name, Doherty J. emphasized the context of the request for identification. In finding that the request amounted to a "seizure" and engaged s. 8 of the *Charter*, he pointed to the fact that the officer's purpose was inherently invasive. In particular, he emphasized that the officer "intended to use that identification *to access a wealth of personal information* about Harris before allowing Harris to proceed on his way."<sup>26</sup>

20. Similarly, the context here supports a conclusion that the police encroach upon a reasonable expectation of privacy when they pierce the anonymity provided by an IP address and ascertain the identity of an Internet user. The Internet has become an established part of modern life. People use the Internet for a great many entirely lawful purposes. The ability to link Internet users to the websites they have visited would reveal a host of intimate details about the user's lifestyle and personal choices. As the Federal Court of Appeal acknowledged, in a case where the music industry was seeking to pierce the anonymity provided by IP addresses to pursue copyright infringement claims,

Citizens legitimately worry about encroachment upon their privacy rights. The potential for unwarranted intrusion into individual personal lives is now unparalleled. In an era where

---

<sup>25</sup> (2007), 225 C.C.C. (3d) 193 (Ont. C.A.).

<sup>26</sup> *Ibid.* at para. 38 (italics added).

people perform many tasks over the Internet, it is possible to learn where one works, resides or shops, his or her financial information, the publications one reads and subscribes to and even specific newspaper articles he or she has browsed. This intrusion not only puts individuals at great personal risk but also subjects their views and beliefs to untenable scrutiny.<sup>27</sup>

The collective understanding that has led members of the public to embrace the Internet for such varied purposes was recognized by Wilkins J., who noted that, “[g]enerally speaking, it is understood that a person's internet protocol address will not be disclosed.”<sup>28</sup> Once it is, as Pringle J. explained in *Cuttell*, it serves to reveal, “intimate details of a subscriber’s lifestyle and choices. Once the police accessed Mr. Cuttell’s name and address, they were able to link his identity to a wealth of intensely personal information.”<sup>29</sup> It is therefore not at all surprising that the Privacy Commissioner of Canada has recommended that basic subscriber information, like the name and address of an Internet user connected to a particular IP address, should only be accessible with a warrant.<sup>30</sup>

21. Those who use the Internet have justifiably come to expect anonymity, as it is essential to shielding their privacy. Should this Honourable Court conclude that Canadians do not enjoy a reasonable expectation of privacy that protects against unwarranted disclosure of an Internet user’s identity, the potential effect on how the Internet is used, especially by those on the social and political margins, could be profound. As Professor Renke has warned,

---

<sup>27</sup> *BMG Canada Inc. v. Doe*, 2005 FCA 193 at para. 4.

<sup>28</sup> *Irwin Toy Ltd. v. Doe*, [2000] O.J. No. 3318 at para. 10 (S.C.J.) (The case involved a plaintiff seeking to compel an Internet Service Provider to disclose the identity of the user behind a particular IP address, in order to pursue a defamation action.)

<sup>29</sup> *Cuttell*, *supra* at para. 21.

<sup>30</sup> See Office of the Privacy Commissioner of Canada, *Customer Name and Address (CNA) Information Consultation Document: Response of the Office of the Privacy Commissioner of Canada to Public Safety Canada*, October 2007, at 6. Available online at: [http://www.priv.gc.ca/information/pub/lar\\_071108\\_e.pdf](http://www.priv.gc.ca/information/pub/lar_071108_e.pdf).

The consequences of this loss of privacy cannot be properly predicted now. If individuals understand that they are constantly under surveillance, a "chilling" effect may occur -- particularly if individuals perceive data mining to be just one of multiple State surveillance techniques. Individuals may constrain their freedoms of belief, expression or association, for fear of generating suspicious patterns.<sup>31</sup>

22. The *CCLA* therefore submits that this Honourable Court should recognize that Internet users do have a reasonable expectation of privacy in information that would reveal their connection to an IP address.

**C. Subsection 7(3)(c.1) of *PIPEDA* Does Not Create a Police Power to Pierce the Anonymity of IP Addresses**

23. The purpose of *PIPEDA*, as explained in s. 3 of the Act, is to:

...establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

Quite obviously, these objectives are entirely complimentary to the purpose underlying section 8 of the *Charter*.

24. To fulfill its purpose, *PIPEDA* requires "organizations"<sup>32</sup> to take positive steps to protect the privacy of "personal information"<sup>33</sup> that they acquire.<sup>34</sup> Those duties, however,

---

<sup>31</sup> Wayne N Renke, "Who Controls the Past Now Controls the Future: Counter-Terrorism, Data Mining and Privacy (2006), 43 *Alta. L. Rev.* 779 at 797. See also Arthur J. Cockfield, "Protecting the Social Value of Privacy in the Context of State Investigations Using New Technologies" (2007), 40 *UBC L. Rev.* 41 at 52.

<sup>32</sup> Defined in s. 2(1) of the Act as including "an association, a partnership, a person and a trade union".

<sup>33</sup> Defined in s. 2(1) of the Act as meaning, "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization".

<sup>34</sup> See *PIPEDA*, s. 5(1) and Schedule 1. Defined in s. 2(1) of the Act as meaning "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization".

are subject to a number of exceptions that are set out in section 7(3) of *PIPEDA*. That subsection provides, in part:

(3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is

\* \* \*

(c) required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records;

(c.1) made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that

(i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs,

(ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, or

(iii) the disclosure is requested for the purpose of administering any law of Canada or a province;

\* \* \*

[Underlining Added]

25. Those lower courts that have concluded that there is no reasonable expectation of privacy in information that would serve to identify an Internet user associated with a particular IP address have invariably pointed to s. 7(3)(c.1) of *PIPEDA* as supplying police with the authority to gain access to such information without first obtaining a warrant. In contrast, those cases that have found a reasonable expectation of privacy in these circumstances have rejected the suggestion that such intrusions can be constitutionally justified under s. 7(3)(c.1).<sup>35</sup>

---

<sup>35</sup> See *supra* note 1.

26. Subsection 7(3)(c.1) must be read in context, in light of the purpose of the overall legislative scheme and the intention of Parliament.<sup>36</sup> To the extent that there is genuine ambiguity, resort may also be had to *Charter* values in choosing between equally plausible interpretations.<sup>37</sup> The purpose of *PIPEDA* is to protect, not undermine, personal privacy, and, as the Honourable John Manley indicated when moving Bill C-6 (*PIPEDA*) for third reading before the House of Commons, the Bill's "law enforcement amendments... allow the status quo to continue and allow businesses to continue to co-operate, where appropriate. These amendments do not grant new powers to government institutions, nor do they create new obligations on business."<sup>38</sup> A more expansive reading of *PIPEDA*'s "law enforcement amendments" would be inconsistent with the intention of Parliament and lead to unconstitutional outcomes.

27. The *CCLA* submits that properly construed, in light of the larger purposes of *PIPEDA*, and the intention of Parliament, as confirmed by the legislative record, the meaning of s. 7(3)(c.1) is readily apparent. The subsection simply lifts the general legal obligation imposed on organizations under the *Act* to keep personal information confidential when they are faced with a government request in which officials have identified their "lawful authority to obtain the information" and indicated that the information is being sought for one of the three permissible purposes enumerated in

---

<sup>36</sup> See *Bell ExpressVu Limited Partnership v. Rex*, [2002] 2 S.C.R. 559 at para. 26. See also *Rizzo & Rizzo Shoes Ltd. (Re)*, [1998] 1 S.C.R. 27 at para. 21.

<sup>37</sup> *Bell ExpressVu*, *supra* at para. 62.

<sup>38</sup> See House of Commons Debates, No. 9 (22 October 1999) at 1015 (Hon. John Manley) [underlining added]. See also *Royal Bank of Canada v. Ren* (2009), 93 O.R. (3d) 43 at para. 22 (Ont.C.A.) (coming to the same conclusion regarding the exceptions found in ss. 7(3)(d)(i) and 7(3)(h.2) of *PIPEDA*, which relate to the banking sector).

subparagraphs (i), (ii) or (iii). Consequently, the subsection does *not* create a police power. Rather, it merely *facilitates* the execution of *existing powers*.

28. In the criminal investigative realm, when police seek access to information that is subject to a reasonable expectation of privacy, absent exigent circumstances, prior judicial approval is constitutionally required.<sup>39</sup> As a result, before *PIPEDA*, when police wanted to access an Internet users' subscriber information they would ordinarily obtain a warrant.<sup>40</sup> In keeping with *PIPEDA*'s "status quo" approach toward law enforcement, this is the standard that should continue to apply in the post-*PIPEDA* world as well. Read in this way, subsections 7(3)(c) and 7(3)(c.1) of *PIPEDA* work in harmony. When police obtain a warrant, they will point to that warrant and bring subsection 7(3)(c) of the Act to the attention of the information holding organization. In such circumstances, it is subsection 7(3)(c) that permits the organization to cooperate without running afoul of its obligations under *PIPEDA*. In those situations where police have the requisite grounds for a warrant but are faced with exigent circumstances that make it impracticable to obtain one, they will point to the relevant statutory provision that expressly authorizes a search in such circumstances,<sup>41</sup> while also bringing subsection 7(3)(c.1) to the organization's attention. In such a scenario, subsection 7(3)(c.1) should assuage any concerns that the organization might otherwise have about cooperating without a court order. Understood in this way, the

---

<sup>39</sup> See *Hunter v. Southam*, *supra* at 109-110.

<sup>40</sup> See *Kwok*, *supra* at para. 34 (the investigating officer in that case testified to this effect).

<sup>41</sup> If the police have the requisite grounds to obtain a warrant but are faced with exigent circumstances that make it impracticable to do so, then they have the express authority to proceed without a warrant. See *Criminal Code*, S.C. 1985, c. C-46, s. 487.11 and *Controlled Drugs and Substances Act*, S.C. 1996, c. 19, s. 11(7).

two subsections achieve Parliament's goal of protecting privacy while also *facilitating* the execution of *existing* police search powers.

**D. Consumer Agreements that Track the Language of the *PIPEDA* Exceptions Should Play No Role In Defining Canadians' Reasonable Privacy Expectations**

29. In many of the cases holding that there was no intrusion upon a reasonable expectation of privacy when police obtained subscriber information linking an Internet user to a particular IP address, the contractual terms contained within agreements between the Internet users and their Internet Service Providers have figured prominently in the courts' analysis.<sup>42</sup> This is true of *Ward*,<sup>43</sup> where one of the contractual terms provided that Bell Sympatico would “disclose any information necessary to satisfy any laws, regulations or other governmental request from any applicable jurisdiction”,<sup>44</sup> and would “offer full cooperation with law enforcement agencies in connection with any investigation” arising from a breach of Bell's “Acceptable Use Policy” (“AUP”).<sup>45</sup> As they did in *Ward*, in almost all of the cases that have dealt with the question currently before this Court, contractual terms such as these were construed as extinguishing any reasonable expectation of privacy that an Internet user might enjoy in the anonymity provided by their IP address. Significantly, however, all of these cases preceded the Supreme Court's recent decision in *Gomboc*.

---

<sup>42</sup> See *Wilson, supra* at para. 43; *Friers, supra* at paras. 21 and 25; *Spencer, supra* at para. 12; *Vasic, supra* at paras. 55-56..

<sup>43</sup> *Ward, supra* at paras. 66-68.

<sup>44</sup> Bell Sympatico Service Agreement, ¶17, Affidavit of T. Burt (Exhibit 2), *Appeal Book in R. v. Ward*, Tab 5B, p. 21 [underlining added].

<sup>45</sup> Bell Sympatico Internet Services – Acceptable Use Policy, Affidavit of T. Burt (Exhibit 2), *Appeal Book in R. v. Ward*, Tab 5B, pp. 26, 28. Among other things, the AUP prohibited subscribers from using their accounts to access or download child pornography.

30. Although *Gomboc* focused on whether the installation of a digital recording ammeter to measure the flow of electricity entering a home encroached upon a reasonable expectation of privacy, so as to engage s. 8 of the *Charter*, the terms of the contractual arrangement between the utility and the customer, which were dictated by a provincial regulation, figured prominently in the Court’s analysis. The regulation entitled the utility to divulge, “customer information” — that is, information “not available to the public” that “is uniquely associated with a customer” — “to a peace officer for the purpose of investigating an offence” so long as “the disclosure is not contrary to the express request of the customer”.<sup>46</sup> Writing for the plurality, Deschamps J. addressed the role of such agreements in assessing the existence of a reasonable expectation of privacy, explaining:

[33] That [the utility] was at liberty to disclose the information weighs heavily against giving the asserted expectation of privacy constitutional recognition. However, in view of the multitudinous forms of information that are generated in customer relationships and given that consumer relationships are often governed by contracts of adhesion (while noting that in this case Mr. Gomboc was at liberty to prevent the disclosure but did not elect to do so), there is every reason for proceeding with caution when deciding what independent constitutional effect disclosure clauses similar to those in the Code of Conduct Regulation may have on determining a reasonable expectation of privacy.

[34] Even if the regulation had been silent on disclosure of energy consumption, the quality and nature of the information disclosed to the police would nonetheless have informed the totality of the circumstances surrounding the expectation of privacy. Determining the expectation of privacy requires examination of whether disclosure involved biographical core data, revealing intimate and private information for which individuals rightly expect constitutional privacy protection. This is consistent with Binnie J.’s comment in *Tessling* that the expectation of privacy is a “normative rather than a descriptive standard” (para. 42). Thus, the fact that the person claiming an expectation of privacy in information ought to have known that the terms governing the relationship with the holder of that information allowed disclosure may not be determinative. Rather, the appropriate question is whether the information is the sort that society accepts should remain out of the state’s hands because of what it reveals about the person involved, the reasons why it was collected, and the circumstances in which it was intended to be used.<sup>47</sup>

<sup>46</sup> *Gomboc*, *supra*, at paras. 83-84, Abella J. concurring.

<sup>47</sup> *Gomboc*, *supra* at paras. 33-34, Deschamps J. concurring (joined by Charron, Rothstein and Cromwell JJ.) (underlining added).

31. Consequently, the fact that a statute or contract permits disclosure to police will not necessarily mean that s. 8 is not engaged. As Chief Justice McLachlin and Justice Fish stated in *Gomboc*, “legislation is only one factor that is to be considered when determining whether an expectation of privacy is objectively reasonable and it may be insufficient to negate an expectation of privacy that is otherwise particularly compelling.”<sup>48</sup> The same is true of commercial contracts of adhesion, such as those at issue in these appeals, which cannot be read as single-handedly subverting otherwise valid privacy expectations.

32. Contractual terms between Internet users and Internet Service Providers have figured prominently when the issues raised by these appeals have been litigated in the courts below, as happened in *Ward*. However, in the aftermath of *Gomboc*, such contractual provisions must be put in their proper context when assessing the “totality of circumstances”. It must be recognized that these sorts of terms have become pervasive *because of PIPEDA*. Section s. 5(1) of the *PIPEDA* requires every organization to “comply with the obligations set out in Schedule 1” of the Act, and that schedule mandates that organizations must disseminate to their clients and customers information about their privacy policies and procedures,<sup>49</sup> including information about the circumstances in which personal information may be disclosed.<sup>50</sup> It is therefore not at all surprising that many of the contractual terms between Internet users and Internet Service Providers serve to roughly track the various exceptions, to the duty owed to keep personal information confidential, that have been carved out by s. 7(3) of *PIPEDA*. Consequently, the terms

---

<sup>48</sup> *Gomboc*, *supra* at para. 115, McLachlin C.J. and Fish J., dissenting.

<sup>49</sup> *PIPEDA*, Schedule 1, 4.1.4(d).

<sup>50</sup> *PIPEDA*, Schedule 1, 4.8.

found in these sorts of agreements should not be construed so as to defeat an Internet user's reasonable expectations of privacy in information that would reveal their connection to an IP address and serve to expose their surfing and browsing activities while online to state scrutiny. It would be most ironic if contractual terms that have effectively been mandated by *PIPEDA*, legislation that was intended to protect privacy, were to ultimately serve to defeat it.

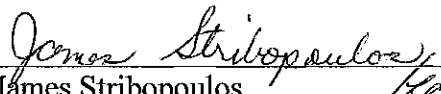
33. The Supreme Court in *Gomboc* specifically recognized the danger of allowing the fine print found in contracts of adhesion to define Canadians' reasonable privacy expectations. In reality, few users take the time to read or have the legal training to fully understand such agreements. Ultimately, as the Supreme Court noted in *Gomboc*, the scope of Canadians' reasonable privacy expectations is a normative constitutional question that cannot be prescribed by statute or defined by contract.<sup>51</sup> As a result, contractual terms that mimic the exceptions found in s. 7(3) of *PIPEDA* should play no role in defining the scope of Canadians' privacy expectations when it comes to their use of the Internet.

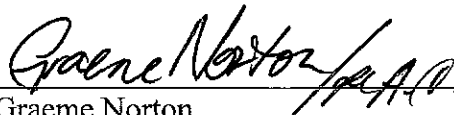
#### **PART IV – ORDER REQUESTED**

34. The *CCLA* respectfully requests that these appeals be allowed.

ALL OF WHICH IS RESPECTFULLY SUBMITTED.

Dated at Toronto this 31<sup>st</sup> day of May, 2011.

  
James Stribopoulos  
Counsel for the Intervener

  
Graeme Norton  
Counsel for the Intervener

<sup>51</sup> *Gomboc*, *supra* at paras 34, 115. See also *Tessling*, *supra* at para. 42; *Patrick*, *supra* at para. 14.

**SCHEDULE A  
TABLE OF AUTHORITIES**

**Cases:**

- R. v. Kwok*, [2008] O.J. No. 2414 (C.J.)
- Re C.(S.)*, [2006] O.J. No. 3754 (C.J.)
- R. v. Friers*, [2008] O.J. No. 5646 (C.J.)
- R. v. Wilson*, [2009] O.J. No. 1067 (S.C.J.)
- R. v. Vasic* (2009), 185 C.R.R. (2d) 286 (Ont. S.C.J.)
- R. v. McGarvie*, 2009 CarswellOnt 500 (C.J.)
- R. v. Verge*, 2009 CarswellOnt 501 (C.J.)
- R. v. Brousseau* (2010), 264 C.C.C. (3d) 562 (Ont.S.C.J.)
- R. v. Spencer* (2009), 361 Sask.R. 1 (Q.B.)
- R. v. Trapp* (2009), 330 Sask. R. 169 (Prov. Ct.)
- R. v. McNeice*, [2010] B.C.J. No. 2131 (S.C.)
- R. v. Ward* (2008), 176 C.R.R. (2d) 90 (Ont.C.J.)
- Hunter v. Southam Inc.*, (1984), 14 C.C.C. (3d) 97 (S.C.C.)
- R. v. Wong* (1990) 60 C.C.C. (3d) 460 (S.C.C.)
- R. v. Greffe*, (1990) 55 C.C.C. (3d) 161 (S.C.C.)
- R. v. Dyment* (1988) 45 C.C.C. (3d) 244 (S.C.C.)
- R. v. Kokesch* (1990) 61 C.C.C. (3d) 207 (S.C.C.)
- R. v. Feeney* (1997), 115 C.C.C. (3d) 129 (S.C.C.)
- R. v. Buhay* (2003), 174 C.C.C. (3d) 97 (S.C.C.)
- R. v. A.M.* (2008), 230 C.C.C. (3d) 377 (S.C.C.)

- R. v. Edwards* (1996), 104 C.C.C. (3d) 136 (S.C.C.)
- R. v. Tessling* (2004), 189 C.C.C. (3d) 189 (S.C.C.)
- R. v. Kang-Brown* (2008), 230 C.C.C. (3d) 289 (S.C.C.)
- R. v. Patrick* (2009), 242 C.C.C. (3d) 158 (S.C.C.)
- R. v. Gomboc*, [2010] 3 S.C.R. 211
- R. v. Plant* (1993) 84 C.C.C. (3d) 204 (S.C.C.)
- R. v. Dersch* (1993), 85 C.C.C. (3d) 1 (S.C.C.)
- R. v. Mills* (1999), 139 C.C.C. (3d) 321 (S.C.C.)
- R. v. Law* (2002), 160 C.C.C. (3d) 449 (S.C.C.)
- Schreiber v. Canada (A.G.)*, (1998), 124 C.C.C. (3d) 129 (S.C.C.)
- R. v. Morelli*, [2010] 1 S.C.R. 253
- R. v. Eddy* (1994) 119 Nfld. & PEIR 91 (Nfld. S.C.T.D.)
- R. v. Harris* (2007), 225 C.C.C. (3d) 193 (Ont. C.A.)
- BMG Canada Inc. v. Doe*, 2005 FCA 193
- Irwin Toy Ltd. v. Doe*, [2000] O.J. No. 3318 (S.C.J.)
- Bell ExpressVu Limited Partnership v. Rex*, [2002] 2 S.C.R. 559
- Rizzo & Rizzo Shoes Ltd. (Re)*, [1998] 1 S.C.R. 27
- Royal Bank of Canada v. Ren* (2009), 93 O.R. (3d) 43 (Ont.C.A.)

***Official Documents and Reports:***

House of Commons Debates, No. 9 (22 October 1999) at 1015 (Hon. John Manley)

Office of the Privacy Commissioner of Canada, *Customer Name and Address (CNA) Information Consultation Document: Response of the Office of the Privacy Commissioner of Canada to Public Safety Canada*, October 2007

***Academic Commentary:***

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

Arthur J. Cockfield, "Protecting the Social Value of Privacy in the Context of State Investigations Using New Technologies" (2007), 40 *UBC L. Rev.* 41

**TABLE B**  
**RELEVANT LEGISLATIVE PROVISIONS**

***Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (U.K.), 1982, c. 11:***

8. Everyone has the right to be secure against unreasonable search or seizure.

\* \* \*

24. (1) Anyone whose rights or freedoms, as guaranteed by this Charter, have been infringed or denied may apply to a court of competent jurisdiction to obtain such remedy as the court considers appropriate and just in the circumstances.

(2) Where, in proceedings under subsection (1), a court concludes that evidence was obtained in a manner that infringed or denied any rights or freedoms guaranteed by this Charter, the evidence shall be excluded if it is established that, having regard to all the circumstances, the admission of it in the proceedings would bring the administration of justice into disrepute.

***Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, as amended:***

2. (1) The definitions in this subsection apply in this Part.

\* \* \*

"commercial activity" means any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists.

\* \* \*

"organization" includes an association, a partnership, a person and a trade union.

\* \* \*

"personal information" means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.

"record" includes any correspondence, memorandum, book, plan, map, drawing, diagram, pictorial or graphic work, photograph, film, microform, sound recording, videotape, machine-readable record and any other documentary material, regardless of physical form or characteristics, and any copy of any of those things.

\* \* \*

### Purpose

3. The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

\* \* \*

### Compliance with obligations

5. (1) Subject to sections 6 to 9, every organization shall comply with the obligations set out in Schedule 1.

### Meaning of "should"

(2) The word "should" , when used in Schedule 1, indicates a recommendation and does not impose an obligation.

### Appropriate purposes

(3) An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.

\* \* \*

### Collection without knowledge or consent

7. (1) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may collect personal information without the knowledge or consent of the individual only if

(a) the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way;

(b) it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province;

(c) the collection is solely for journalistic, artistic or literary purposes;

(d) the information is publicly available and is specified by the regulations; or

- (e) the collection is made for the purpose of making a disclosure
  - (i) under subparagraph (3)(c.1)(i) or (d)(ii), or
  - (ii) that is required by law.

#### Use without knowledge or consent

(2) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may, without the knowledge or consent of the individual, use personal information only if

- (a) in the course of its activities, the organization becomes aware of information that it has reasonable grounds to believe could be useful in the investigation of a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, and the information is used for the purpose of investigating that contravention;
- (b) it is used for the purpose of acting in respect of an emergency that threatens the life, health or security of an individual;
- (c) it is used for statistical, or scholarly study or research, purposes that cannot be achieved without using the information, the information is used in a manner that will ensure its confidentiality, it is impracticable to obtain consent and the organization informs the Commissioner of the use before the information is used;
- (c.1) it is publicly available and is specified by the regulations; or
- (d) it was collected under paragraph (1)(a), (b) or (e).

#### Disclosure without knowledge or consent

(3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is

- (a) made to, in the Province of Quebec, an advocate or notary or, in any other province, a barrister or solicitor who is representing the organization;
- (b) for the purpose of collecting a debt owed by the individual to the organization;
- (c) required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records;
- (c.1) made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that
  - (i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs,
  - (ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, or

(iii) the disclosure is requested for the purpose of administering any law of Canada or a province;

(c.2) made to the government institution mentioned in section 7 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* as required by that section;

\*(c.2) made to the government institution mentioned in section 7 of the *Proceeds of Crime (Money Laundering) Act* as required by that section;

\* [Note: Paragraph 7(3)(c.2), as enacted by paragraph 97(1)(a) of chapter 17 of the Statutes of Canada, 2000, will be repealed at a later date.]

(d) made on the initiative of the organization to an investigative body, a government institution or a part of a government institution and the organization

(i) has reasonable grounds to believe that the information relates to a breach of an agreement or a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, or

(ii) suspects that the information relates to national security, the defence of Canada or the conduct of international affairs;

(e) made to a person who needs the information because of an emergency that threatens the life, health or security of an individual and, if the individual whom the information is about is alive, the organization informs that individual in writing without delay of the disclosure;

(f) for statistical, or scholarly study or research, purposes that cannot be achieved without disclosing the information, it is impracticable to obtain consent and the organization informs the Commissioner of the disclosure before the information is disclosed;

(g) made to an institution whose functions include the conservation of records of historic or archival importance, and the disclosure is made for the purpose of such conservation;

(h) made after the earlier of

(i) one hundred years after the record containing the information was created, and

(ii) twenty years after the death of the individual whom the information is about;

(h.1) of information that is publicly available and is specified by the regulations;

(h.2) made by an investigative body and the disclosure is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province; or

(i) required by law.

Use without consent

(4) Despite clause 4.5 of Schedule 1, an organization may use personal information for purposes other than those for which it was collected in any of the circumstances set out in subsection (2).

Disclosure without consent

(5) Despite clause 4.5 of Schedule 1, an organization may disclose personal information for purposes other than those for which it was collected in any of the circumstances set out in paragraphs (3)(a) to (h.2).

\* \* \*

SCHEDULE 1

(Section 5)

PRINCIPLES SET OUT IN THE NATIONAL STANDARD OF CANADA ENTITLED MODEL CODE FOR THE PROTECTION OF PERSONAL INFORMATION, CAN/CSA-Q830-96

\* \* \*

4.1.4

Organizations shall implement policies and practices to give effect to the principles, including

- (a) implementing procedures to protect personal information;
- (b) establishing procedures to receive and respond to complaints and inquiries;
- (c) training staff and communicating to staff information about the organization's policies and practices; and
- (d) developing information to explain the organization's policies and procedures.

\* \* \*

4.8 Principle 8 — Openness

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

4.8.1

Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This

information shall be made available in a form that is generally understandable.

#### 4.8.2

The information made available shall include

- (a) the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;
- (b) the means of gaining access to personal information held by the organization;
- (c) a description of the type of personal information held by the organization, including a general account of its use;
- (d) a copy of any brochures or other information that explain the organization's policies, standards, or codes; and
- (e) what personal information is made available to related organizations (e.g., subsidiaries).

#### 4.8.3

An organization may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, an organization may choose to make brochures available in its place of business, mail information to its customers, provide online access, or establish a toll-free telephone number.

\* \* \*

#### ***Criminal Code, S.C. 1985, c. C-46, as amended:***

**487.11** A peace officer, or a public officer who has been appointed or designated to administer or enforce any federal or provincial law and whose duties include the enforcement of this or any other Act of Parliament, may, in the course of his or her duties, exercise any of the powers described in subsection 487(1) or 492.1(1) without a warrant if the conditions for obtaining a warrant exist but by reason of exigent circumstances it would be impracticable to obtain a warrant.

#### ***Controlled Drugs and Substances Act, S.C. 1996, c. 19:***

**11(7)** A peace officer may exercise any of the powers described in subsection (1), (5) or (6) without a warrant if the conditions for obtaining a warrant exist but by reason of exigent circumstances it would be impracticable to obtain one.