Court File No. 34644

IN THE SUPREME COURT OF CANADA

(ON APPEAL FROM THE COURT OF APPEAL FOR SASKATCHEWAN)

B E T W E E N

MATTHEW DAVID SPENCER

APPELLANT
(Appellant/Respondent)

– and –

HER MAJESTY THE QUEEN

RESPONDENT
(Respondent/Appellant)

– and –

ATTORNEY GENERAL OF ALBERTA, ATTORNEY GENERAL OF ONTARIO CANADIAN CIVIL LIBERTIES ASSOCIATION, CRIMINAL LAWYERS' ASSOCIATION OF ONTARIO, DIRECTOR OF PUBLIC PROSECUTIONS OF CANADA, PRIVACY COMMISSIONER OF CANADA

INTERVENERS

FACTUM OF THE INTERVENER CRIMINAL LAWYERS' ASSOCIATION OF ONTARIO

(Pursuant to Rule 42 of the *Rules of the Supreme Court of Canada*)

SCHRECK PRESSER LLP
5th Flr., 6 Adelaide St. E.
Toronto, ON M5C 1H6

Jill R. Presser
Tel.: (416) 586-0330
Fax: (416) 977-8513
Email: presser@schreckpresser.com

DAWE DINEEN
171 John Street, Suite 101
Toronto, ON M5T 1X3

Jonathan Dawe
Tel.: (416) 649-5058
Fax: (416) 352-7733
Email: jdawe@dawedineen.com

Counsel for the Intervener, Criminal Lawyers' Association of Ontario

SUPREME ADVOCACY LLP
397 Gladstone Ave., Suite 100
Ottawa, ON K2P 0Y9

Marie-France Major
Tel.: (613) 695-8855
Fax: (613) 695-8580
Email: mfmajor@supremeadvocacy.ca

Ottawa Agent for Counsel for the Intervener, Criminal Lawyers' Association of Ontario

MCDOUGALL GAULEY LLP
1500 - 1881 Scarth Street
Regina, SK S4P 4K9

Aaron A. Fox, Q.C.
Darren K. Kraushaar
Tel.: (306) 565-5147
Fax: (306) 359-0785
Email: afox@mcdougallgauley.com

Counsel for the Appellant, Matthew David Spencer

MCMILLAN LLP
50 O'Connor Street, Suite 300
Ottawa, ON K1P 6L2

Jeffrey W. Beedell
Tel.: (613) 232-7171
Fax: (613) 231-3191
Email: jeff.beedell@mcmillan.ca

Ottawa Agent for Counsel for the Appellant, Matthew David Spencer

ATTORNEY GENERAL FOR SASKATCHEWAN
1874 Scarth Street, 3rd Floor
Regina, SK S4P 4B3

Anthony B. Gerein
Tel.: (306) 787-5490
Fax: (306) 787-8878
Email: tony.gerein@gov.sk.ca

Counsel for Respondent Her Majesty the Queen

GOWLING LAFLEUR HENDERSON LLP
2600 - 160 Elgin St
Ottawa, Ontario, K1P 1C3

Henry S. Brown, Q.C.
Tel.: (613) 233-1781
Fax: (613) 788-3433
Email: henry.brown@gowlings.com

Ottawa Agent for Counsel for Respondent Her Majesty the Queen

ATTORNEY GENERAL OF ALBERTA
3rd Floor, Centrium Place
300, 332 - 6 Avenue S.W.
Calgary, AB T2P 0B2

Jolaine Antonio
Tel.: (403) 592-4902
Fax: (403) 297-3453
Email: jolaine.antonio@gov.ab.ca

Counsel for the Intervener, Attorney General of Alberta

GOWLING LAFLEUR HENDERSON LLP
2600 - 160 Elgin St
Ottawa, Ontario, K1P 1C3

Brian A. Crane, Q.C.
Tel.: (613) 233-1781
Fax: (613) 563-9869
Email: brian.crane@gowlings.com

Ottawa Agent for Counsel for the Intervener, Attorney General of Alberta

PUBLIC PROSECUTION SERVICE OF CANADA
700 EPCOR Tower 10423, 101st Street
Edmonton, AB T4H 0E7

Ronald C. Reimer
Tel.: (780) 495-4079
Fax: (780) 495-6940
Email: ron.reimer@ppsc-sppc.gc.ca

Counsel for Intervener, Director of Public Prosecutions

DIRECTEUR DES POURSUITES PÉNALES DU CANADA
284, rue Wellington, 2ième étage
Ottawa, ON K1A 0H8

François Lacasse
Tel.: (613) 957-4770
Fax: (613) 941-7865
Email: flacasse@ppsc-sppc.gc.ca

Ottawa Agent for Counsel for Intervener, Director of Public Prosecutions

ATTORNEY GENERAL OF ONTARIO
Crown Law Office, Criminal
720 Bay Street, 10th Floor
Toronto, ON M5G 2K1

Susan Magotiaux
Alison Dellandrea
Tel.: (416) 326-5238
Fax: (416) 326-4656
Email: susan.magotiaux@ontario.ca

Counsel for Intervener, Attorney General of Ontario

BURKE-ROBERTSON
441 MacLaren Street, Suite 200
Ottawa, ON K2P 2H3

Robert E. Houston, Q.C.
Tel.: (613) 236-9665
Fax: (613) 235-4430
Email: rhouston@burkerobertson.com

Ottawa Agent for Counsel for Intervener, Attorney General of Ontario

KAPOOR BARRISTERS
20 Adelaide Street East, Suite 210
Toronto, ON M5C 2T6

James Stribopoulos
Tel.: (416) 363-2700
Fax: (416) 368-6811
Email: jst@kapoorbarristers.com

Counsel for Intervener, Canadian Civil Liberties Association

GREENSPON, BROWN & ASSOCIATES
331 Somerset Street West
Ottawa, ON K2P 0J8

Lawrence Greenspon
Tel.: (613) 288-2890
Fax: (613) 288-2896
Email: email@lgreenspon.com

Ottawa Agent for Counsel for Intervener, Canadian Civil Liberties Association

OSLER, HOSKIN & HARCOURT LLP
Box 50, 1 First Canadian Place
Toronto, ON M5X 1B8

Mahmud Jamal
Sarah Speevak
Tel.: (416) 862-6764
Fax: (416) 862-6666
Email: mjamal@osler.com

Counsel for the Intervener, Privacy Commissioner of Canada

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA
112 Kent Street, 3rd Floor
Place de Ville, Tower B
Ottawa, ON K1A 1H3

Daniel Caron
Patricia Kosseim
Tel.: (613) 947-4634
Fax: (613) 947-4192
Email: daniel.caron@priv.gc.ca

Ottawa Agent for Counsel for the Intervener, Privacy Commissioner of Canada

TABLE OF CONTENTS

PART I: STATEMENT OF FACTS

1. The CLA accepts the facts as summarized in the parties' facta.

PART II: THE CLA'S POSITION ON THE QUESTIONS IN ISSUE

2. This appeal will decide whether s. 8 of the Charter requires the police to obtain judicial authorization to gain access to internet service providers' records of their assignment of internet protocol addresses to subscribers. The CLA's position is that in view of the growing societal importance of the internet Canadians' online privacy deserves strong s. 8 *Charter* protection. An internet service provider's records of its IP address assignments are like a cipher key that unlocks internet privacy by linking individual subscribers to particular IP addresses on specific occasions. Someone armed with this information can easily learn details of a person's activities on the internet, which can be extremely revealing. Access to this information should therefore be judicially regulated under s. 8 and the police should not be able to obtain it without a warrant. The CLA's submits further that:

i) "Privacy" for s. 8 *Charter* purposes should be recognized as including the ability to move about anonymously in public spaces, including the more public parts of cyberspace;

ii) Neither *PIPEDA*[1] nor s. 487.014 of the *Criminal Code* create warrantless search and seizure powers, and neither authorize the police to make warrantless production requests for s. 8 *Charter*-protected information in the hands of third party businesses;

iii) Courts should "proceed with caution"[2] when assessing the impact on *Charter* rights of terms buried in standard-form contracts of adhesion, bearing in mind how few consumers actually read or fully understand these documents and taking into account the legal backdrop of privacy protections created by *PIPEDA* and the *Charter*;

iv) Since *Charter* privacy issues must be "framed in broad and neutral terms",[3] s. 8 protection cannot be seen to ebb and flow with the type of offence being investigated;

v) Agreements between police agencies and private businesses are not "law" and cannot override s. 8 *Charter* protections.

The CLA adopts the submissions of the Canadian Civil Liberties Association and the Privacy Commissioner of Canada and to avoid repetition will not address all of the above points in

---

[1] The *Personal Information Protection and Electronic Documents Act*, S.C. 2000.
[2] *R. v. Gomboc*, [2010] 3 S.C.R. 211, 2010 SCC 55, at ¶33, *per* Deschamps J., concurring.
[3] See *R. v. Wong*, [1990] 3 S.C.R. 36 at p. 50; *R. v. Buhay*, [2003] 1 S.C.R. 631, 2003 S.C.C. 30 at ¶19*; R. v. M.(A.)*, [2009] 1 S.C.R. 569, 2008 S.C.C. 19 at ¶70.

detail.[4] The CLA takes no position on the other legal issues raised by the Appellant[5] or on the disposition of this appeal.

PART III: ARGUMENT

A. Overview

3. This is a watershed moment for the right to privacy. Breakthroughs in computing and communications technology have dramatically changed how Canadians live their day-to-day lives. For most people using the internet has become a practical necessity, both professionally and socially.[6] Anyone going online inevitably exposes highly sensitive personal information to the third party businesses who act as the internet's gatekeepers and managers. The plummeting cost of digital storage allows vast quantities of this information to be stored indefinitely.[7] In combination, these technological and social developments present new and in many respects unparalleled threats to Canadians' personal privacy. More than two decades ago, in *R. v. Wong, infra,* La Forest J. declared that "the broad and general right to be secure from unreasonable search and seizure guaranteed by s. 8 [of the *Charter*] is meant to keep pace with technological development."[8] This Court must now give practical effect to this principle.

4. Few Canadians have the expertise to understand fully how the internet works at a technical level or to grasp all the different ways their online activities put their privacy at risk. Moreover, hardly anyone who "clicks to accept" a multi-page "user agreement" to get internet access actually reads it first, let alone fully comprehends how it may affect their privacy. Canadians nevertheless overwhelmingly believe that their on-line activities *should* be private and not subject to unregulated government surveillance.[9] This Court has repeatedly declared that

---

[4] In particular, the CLA relies entirely on the CCLA and the Privacy Commissioner's submissions in relation to points ii) and iii), above.

[5] Specifically, the CLA takes no position on whether the evidence seized in the Appellant's case should be excluded under s. 24(2) or on whether the Saskatchewan Court of Appeal erred by overturning his acquittal at trial on the "make available" count.

[6] In this regard, an analogy can be drawn with Iacobucci J.'s comments in his majority decision in *R. v. White,* [1999] 2 S.C.R. 417 at ¶55, describing driving a motor vehicle as activity that is "not freely undertaken in precisely the same way as one is free to participate in a regulated industry such as the commercial fishery" but as something that is "often a necessity of life".

[7] Thirty years ago it would have cost several hundred thousand dollars to buy sufficient hard drive space to store a gigabyte (10^9 bytes) of data. The cost is now less than a dime.

[8] *R. v. Wong,* [1990] 3 S.C.R. 36 at p. 44; see also *R. v. Tessling,* [2004] 3 S.C.R. 432, 2004 S.C.C. 67 at ¶54-55.

[9] For instance, in a 2004 public opinion survey commissioned by the Public Interest Advocacy Centre, 86% of respondents agreed that the government should not be able to "monitor your Internet use without a warrant". (Public

"[e]xpectation of privacy is a normative rather than a descriptive standard".[10] In *R. v. M.(A.)*, *supra*, Binnie J., writing for the majority on this point, stated:

> Section 8, like the rest of the *Charter*, must be interpreted purposively, that is to say, to further the interests it was intended to protect. … A privacy interest worth of protection is one the citizen subjectively believes ought to be respected by government and "that society is prepared to recognize as 'reasonable'".[11]

The fundamental question at issue in this appeal is whether the *Charter* will be interpreted to provide the privacy protection Canadians think they should have.

5. Although the specific police request for information at issue here was relatively narrow, the implications of the Respondent's arguments for why the police did not need a warrant are far-reaching. If accepted, they would create a legal regime in which the disclosure of information capable of revealing details of Canadians' internet activities is entirely unregulated by the *Charter* and left solely up to the discretion of private companies acting in consultation with the police. The CLA's position is that the growing role of the internet in Canadian society makes issues of online privacy far too important to be decided in this haphazard fashion. Rather, a purposive approach to s. 8 of the *Charter* demands that this information be recognized as private and that state access to it be subjected to judicial control. The *Charter* has given this Court responsibility for ensuring that the privacy essential in a free and democratic society is preserved even as digital technology becomes increasingly interwoven into the fabric of Canadian life.

B. Identifying the privacy interest at stake

6. In *R. v. Morelli, infra* this Court recognized the high degree of privacy associated with "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."[12] The web pages one visits and the internet searches one conducts very often reveal intimate details about one's health, finances, politics, social and sexual relationships and other intensely personal matters. Section 8 of the *Charter* is clearly engaged when the police get this information directly

---

Interest Advocacy Centre, *Consumer Privacy and State Security: Losing our Balance*, November, 2004, at pp. 29-30, 48). See also *BMG Canada Inc. v. Doe*, 2005 FCA 193 at ¶4; *Irwin Toy Ltd. v. Doe*, [2000] O.J. No. 3318 at ¶10-11 (S.C.J.).

[10] *R. v. Tessling*, *supra*, at ¶42; *R. v. M.(A.)*, *supra*, at ¶33; *R. v. Patrick*, [2009] 1 S.C.R. 579, 2009 S.C.C. 17 at ¶12; *R. v. Gomboc*, 2010 S.C.C. 55, [2010] 3 S.C.R. 211 at ¶34, *per* Deschamps J., at ¶115, *per* McLachlin C.J.C. and Fish J. (dissenting in the result).

[11] *R. v. M.(A.)*, *supra* at ¶33, quoting from the United States Supreme Court decision in *United States v. Katz*, 389 U.S. 347 (1967). See also *R. v. Wong*, *supra* at p. 50; *R. v. Patrick*, *supra* at ¶14.

[12] *R. v. Morelli*, [2010] 1 S.C.R. 253, 2010 S.C.C. 8 at ¶2-3.

from a personal computer. The central policy issue in this appeal is whether the *Charter* should also regulate police efforts to reconstruct the "electronic roadmap" of a person's "cybernetic peregrinations" from information stored in the digital files of third party ISPs.

7. Internet users must have a unique "internet protocol address", which most people obtain from a commercial internet service provider. The online activities of particular IP addresses are regularly logged and recorded and can be obtained in various ways by third parties, including the police. This information is often highly revealing.[13] The existence of privacy on the internet depends on the fact that without more it is difficult to link the "cybernetic peregrinations" of an IP address to the activities of a particular person. The extra information needed to make this connection can be found in the ISP's records detailing how it has allocated its IP addresses to its subscribers over time. Contrary to the Respondent's repeated assertion, these ISP records reveal more than merely subscribers' names and addresses and the unremarkable fact that they get internet service from a certain provider. Rather, the contents of these databases is like a cipher key that unlocks internet privacy by enabling the activities of particular IP addresses on specific dates and times to be linked to individual subscribers[14] – which is of course precisely why the police want it. Researchers for the Privacy Commissioner of Canada have concluded that:

> … unlike simple phone book information, the elements examined [*i.e.*, the information in ISPs' subscriber information databases] can be used to develop very detailed portraits of individuals providing insight into one's activities, tastes, leanings and lives.[15]

The critical question this Court must decide is whether s. 8 the *Charter* should be understood to regulate state access to this information.

8. The cases that have considered this issue to date have all involved very similar fact patterns.[16] This is not coincidental. Rather, it results from a deal between the largest Canadian

---

[13] For instance, when given a particular IP address researchers from the Office of the Privacy Commissioner of Canada were able to determine that someone using that address had edited numerous Wikipedia pages on specific topics, had conducted "an online search for a specific type of person" and had followed this up by visiting "a site devoted to sexual preferences". See "What an IP Address Can Reveal About You" (May, 2013), BOOK OF AUTHORITIES OF THE INTERVENER PRIVACY COMMISSIONER OF CANADA, TAB 35).

[14] See *R. v. Trapp*, 2011 SKCA 143 at ¶35, per Cameron J.A.; *R. v. Ward*, 2012 ONCA 660 at ¶67-69

[15] "What an IP Address Can Reveal About You" (May, 2013), *supra*.

[16] In addition to the case at bar, the companion case *R. v. Trapp*, *supra* and the Ontario Court of Appeal's decision in *R. v. Ward*, *supra*, trial-level decisions on this issue include.: *R. v. Cuttell* (2009), 247 C.C.C. (3d) 424 (Ont. C.J.); *R. v. F.(S.W.)*, 2008 ONCJ 740; *R. v. Wilson*, 2009 O.J. No. 1067 (S.C.J.); *R. v. Vasic*, 2009 CanLII 6842 (Ont. S.C.J.); *R. v. McGarvie*, 2009 CarswellOnt 500 (C.J.); *R. v. Verge*, 2009 CarswellOnt 501 (C.J.); *R. v. Brousseau*, 2010 ONSC 6753; *R. v. Kwok*, [2008] O.J. No. 2414 (S.C.J.); *Re C.(S.)*, [2006] O.J. No. 3754 (C.J.); *R. v. McNeice*, 2010 BCSC 1544.

ISPs and the police that governs how these ISPs respond to warrantless police requests.[17] Participating ISPs will give the police warrantless access to information from their IP address allocation databases only in certain limited circumstances: (i) the police must assert that they are investigating a "child sexual exploitation offence", which in practice almost invariably means a child pornography offence; and (ii) the request must be in the form of a request for the identity of the subscriber who was assigned a particular IP addresses on a specific occasion. In all other situations the ISPs treat the contents of their IP address assignment databases as private and not disclosable to the police without a warrant.[18] However, Professors Slane and Austin note:

> [C]ompanies agreeing to participate … verified that their subscriber agreements indicated that they would cooperate with such requests from law enforcement, or changed them so that they did. Because changing subscriber agreements is costly, companies sometimes chose to phrase their willingness to cooperate quite broadly so as to avoid having to revise again, even though in practice it is only in child exploitation investigations that the companies have so far chosen to forego requiring a warrant.[19]

9. If the Respondent's view of the law prevails, the current limits on what most ISPs will give the police without a warrant are gratuitous self-imposed constraints they could abandon any time with no legal repercussions. The correctness of this contention ultimately hinges on whether or not the information at issue engages s. 8 of the *Charter*.[20] If there is no privacy in IP address allocation information there would seemingly be no legal impediment to an ISP giving the police

---

[17] 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 C.LQ. 486; S. Morin, "Updated: Business Disclosure of Personal Information to Law Enforcement Agencies: PIPEDA and the CNA Letter of Request Protocol", *Privacy Pages: CBA National and Privacy Access Law Section Newsletter* (November 2011).

[18] For instance, these ISPs would not give the police a list of all the IP addresses assigned to a particular subscriber over some time period, and would decline to provide any information without a warrant if the police indicated they were investigating something other than a "child sexual exploitation offence".

[19] Slane and Austin, *supra* at p. 486. In the case at bar Shaw's "Acceptable Use Policy" ("AUP") refers to Shaw's willingness to cooperate with "the investigation of suspected criminal violations", even though most ISPs will apparently only provide IP address allocation information to the police without a warrant when the police indicate they are investigating a child sexual exploitation offence.

[20] For instance, in the case at bar: (i) Shaw's "Acceptable Use Policy" ("AUP") authorizes Shaw to "cooperate with law enforcement authorities in the investigation of suspected criminal violations" by "providing the username, IP address or other identifying information about a subscriber", but only if this is done "in accordance with the guidelines set out in Shaw's Privacy Policy"; (ii) Shaw's "Privacy Policy" authorizes Shaw to disclose information to the police only "as permitted by law", including *PIPEDA;* (iii) *PIPEDA* authorizes ISPs to make warrantless disclosures to the police only when the police have "lawful authority to obtain the information"; (iv) a police request for information that attracts a "reasonable expectation of privacy" is a "search" for s. 8 *Charter* purposes (see, *e.g., R. v. Plant,* [1993] 3 S.C.R. 281 at pp. 291-96; *R. v. Law,* [2002] 1 S.C.R. 227, 2002 S.C.C. 10 at ¶15); (v) warrantless searches violate s. 8 unless they are specifically "authorized by law"; (vi) Neither *PIPEDA* nor s. 487.014 of the *Criminal Code* create a warrantless search power (see the factum of the Privacy Commissioner of Canada at ¶10-16). Putting all of these pieces together, if the information at issue in the case at bar engaged s. 8 of the *Charter* its warrantless disclosure to the police on their request was contrary to the *Charter,* in breach of *PIPEDA* and apparently also unauthorized by the terms of the subscription contract.

wholesale access to its entire database of IP address assignments for all subscribers and all times, nor would the *Charter* bar the police from requesting this information on the off chance it might prove useful in the future. It is also implicit in the Respondent's position that a law compelling ISPs to grant the police broader warrantless access to their IP address assignment databases[21] would not infringe s. 8 or require s. 1 justification. The CLA's position is that such a legal regime would provide grossly inadequate protection for Canadians' internet privacy.

C. Privacy and anonymity in public spaces

10. Some online activities are conducted without anonymity but with a strong expectation that they will be private.[22] However, casual web browsing is usually done anonymously. For instance, people who go to medical information websites to research health conditions ordinarily do not provide their names and expect their visit to remain unknown to the world at large.

11. Analogies between cyberspace and physical space are often inexact and must be approached with caution. It is tempting to compare web sites to physical places and analogize "surfing the web" to travelling around on public roads. This analogy can be misleading since the internet is in many ways far less "public" than the streets. However, some web sites – for example, internet forums and discussion boards – are modeled after traditional public spaces and encourage visitors to participate in public online discussion. On many such sites it is nevertheless the established social norm for participants to use pseudonyms and keep their true identities hidden. This raises an important point of law: does "privacy" for s. 8 *Charter* purposes include the ability to be anonymous in public spaces, both real and virtual?

12. In *R. v. Wise* this Court found s. 8 of the *Charter* to be engaged by the electronic tracking of a target's physical movements in public, holding that "the installation of the [tracking] device [in the target's vehicle] and its subsequent use to monitor the vehicle, together, constituted the unreasonable search."[23] However, the majority judgment did not address in detail the issue of

[21] The controversial and now-withdrawn "lawful access" bill (Bill C-30) would have done just that.
[22] Examples include sending emails, banking online or making an online credit card purchase.
[23] *R. v. Wise*, [1992] 1 S.C.R. 527 at p. 538, *per* Cory J.

privacy in public places,[24] while La Forest J.'s extensive discussion of the point was written for himself alone, dissenting in the result.[25]

13. There have been two noteworthy developments since *Wise*. First, in *R. v. Ward, supra* the Ontario Court of Appeal expanded on this Court's holding in *Wise,* construing the decision as recognizing a conception of s. 8 "privacy" that includes the ability to enjoy anonymity in public spaces. The CLA cannot improve on Doherty J.A.'s analysis at paras. 70-75 of his reasons and respectfully adopts it.

14. Second, in its 2012 decision in *United States v. Jones*[26] a majority of justices of the United States Supreme Court indicated their willingness to reconsider its prior holding in *United States v. Knotts* that a person moving about in public "has no reasonable expectation of privacy in his movements from one place to another".[27] The police in *Jones*, acting without a warrant, had installed a GPS tracking device (much more sophisticated than the simple "beeper" in *Wise*) on the undercarriage of Jones's vehicle and used it to record his movements for the next four weeks. Although a majority of the Court (*per* Scalia J.[28]) decided the case on the narrow basis that the initial installation of the device violated the Fourth Amendment, four concurring justices, led by Alito J.,[29] would have decided the case on the basis that "the use of longer term GPS monitoring in investigations for most offenses impinges on expectations of privacy".[30] Moreover, Sotomayor J. joined the majority but also wrote a separate concurrence endorsing Alito J.'s privacy analysis and indicating her willingness to go even further.[31] Of particular importance to the case at bar, Sotomayor J. raised the issue of privacy on the internet and stated

---

[24] The Crown had conceded in this Court that the installation of the tracking device violated s. 8 *Charter*, so the main focus of the majority's decision was on whether or not the evidence obtained should be excluded under s. 24(2).
[25] See *Wise, supra* at pp. 556-66.
[26] 536 US ___, 132 S.Ct. 945 (2012)
[27] *United States v. Knotts*, 460 U.S. 276 at p. 281 (1983)
[28] Joined by Roberts C.J. and Kennedy, Thomas, and Sotomayor JJ.
[29] Joined by Ginsburg, Breyer and Kagan JJ.. These justices expressly disagreed with the majority's holding that the initial installation of the device was a "search" for Fourth Amendment purposes and thus relied exclusively on the subsequent police monitoring of Jones's movements as establishing the Fourth Amendment violation in the case.
[30] Slip opinion at p. 13. Alito J. interpreted *Knotts* as concerned only with "relatively short-term monitoring of a person's movements on public streets", but did not indicate the precise location of the line between permissible "short-term" and impermissible "long-term" monitoring, stating: "[w]e need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark".
[31] Sotomayor J. agreed with Alito J. that the Fourth Amendment was engaged "at the very least" by "longer term GPS monitoring" but strongly should that even shorter-term monitoring would be constitutionally problematic having regard to the "unique attributes" of GPS surveillance.

that in view of technological developments "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties". This latter premise – the long-established US "risk analysis" doctrine – provides the legal foundation for the American decisions referred to by the Respondent[32] in support of its claim that no expectation of privacy should be recognized in IP address assignment information. This Court has consistently refused to adopt the US "risk analysis" doctrine s. 8 *Charter* cases, and Sotomayor J.'s *Jones* concurrence persuasively explains why "[t]his approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[33]

D. Privacy issues must be "framed in broad and neutral terms"

15. This Court has repeatedly held that the normative question of whether to recognize a reasonable expectation of privacy in a specific context must be decided on the basis of questions "framed in broad and neutral terms".[34] As La Forest J. explained in *R. v. Wong*, *supra*:

> [T]the answer to the question whether persons who were the object of [a search] had a reasonable expectation of privacy cannot be made to depend on whether or not those persons were engaged in illegal activities …

In the case at bar, the focus must thus be on the privacy expectations of internet subscribers in general, not merely the small subset who use the internet for illegal purposes. Further, as noted above, this Court has also consistently declined to adopt the US "risk analysis" doctrine, under which the voluntary disclosure of information to a third party is deemed to destroy privacy based on the risk that the third party might divulge it to state authorities. In *R. v. Cole* this Court rejected the closely-related American doctrine of third-party consent, which Fish J. explained:

> … is premised on the notion that third party consent is justifiable because the individual voluntarily assumed the risk that his information would fall into the hands of law enforcement. … However, this Court rejected that sort of "risk analysis" in *R. v. Duarte* [*infra*].
>
> Moreover, the doctrine of third party consent is inconsistent with this Court's jurisprudence on *first party* consent.[35]

Accordingly, if information otherwise qualifies as "private" for s. 8 *Charter* purposes it does not lose this status merely because the records-holder in a given case chose to give it to the police.

---

[32] At ¶102 of its factum.
[33] *Jones*, *supra*, per Sotomayor J, at p. 5.
[34] See, *e.g.*, *R. v. Wong*, *supra*, *R. v. Buhay*, [2003] 1 S.C.R. 631, 2003 S.C.C. 30*; R. v. A.M.*, *supra.*
[35] *R. v. Cole*, [2012] 3 S.C.R. 34, 2012 S.C.C. 53 at ¶76-77; citing *R. v. Duarte*, [1990] 1 S.C.R. 30 at pp. 39-54

16. In *R. v. Ward, supra,* Doherty J.A. introduced two novel – and, the CLA submits, unwelcome – factors into his s. 8 *Charter* privacy analysis. First, he held that:

> The normative nature of the reasonable expectation of privacy analysis and the value judgments that underlie that analysis require that [the ISP's] legitimate interests, whether described as self-interest, civic engagement, or both, be taken into account in determining whether the appellant had a reasonable expectation of privacy in respect of the information held by [the ISP].[36]

Second, he held that the ISP "was entitled to have regard to the nature of the offences being investigated when it decided whether to disclose the information." Doherty J.A. maintained that this approach avoided "fall[ing] into the trap of judging the appellant's privacy expectation by reference to the nature of his activity" because it treated the offence under investigation as only "relevant to the reasonableness of [the ISP's] response to the police request".[37]

17. The CLA submits that despite Doherty J.A.'s disclaimer, his reliance on these factors conflicts with the firmly established "broad and neutral" approach to privacy. If internet subscribers in general have a s. 8 privacy interest over their IP address assignment histories, their privacy cannot be seen to ebb and flow depending on the ISP's interest in cooperating with the police in a particular case. For instance, in *Wong* the hotel's interest in helping the police stop its rooms from being used for illegal gambling was treated by this Court as irrelevant to the threshold s. 8 privacy analysis, which turned solely on the "broad and neutral" question of whether hotel guests should generally be able to expect privacy in their rooms. Treating a third party's interest in cooperating the police as capable of destroying an otherwise existing privacy interest would also be at odds with this Court's rejection of the "third party consent" doctrine in *Cole, supra*. In effect, Doherty J.A.'s reliance on this factor admits through the back door the "risk analysis" approach this Court has consistently rejected.

18. Moreover, if the *actual* nature of a subscriber's online activities has no bearing on the existence of a reasonable expectation of privacy, it makes little sense to treat an ISP's *belief* that a certain type of crime *may* have been committed as somehow germane to the privacy analysis, particularly when this belief arises from a bare assertion by police that they are investigating a particular offence.[38] The strength of the police grounds to suspect a crime has been committed

---

[36] *Ward, supra* at ¶98.
[37] *Ward, supra* at ¶103.
[38] In this regard, it is important to note that the applicable legal framework is very different in cases an ISP itself finds evidence of subscriber wrongdoing and discloses information to the police on its own initiative rather than at

may be highly relevant to the second branch of s. 8 – whether the state is justified in invading the target's privacy – but under the established analytic framework it has no bearing on the threshold question of whether a protected privacy interest exists in the first place. Indeed, since this Court has held that the seriousness of the offence under investigation has no role at this stage of the analysis,[39] it would be incoherent to treat the nature of the offence as a relevant factor. This incoherence would remain even if this factor were treated as bearing on the "reasonableness" of a third party records-holder's response to a police request, as Doherty J.A. proposes.

19. In essence, the current arrangement between ISPs and the police reflects the participating ISPs' belief that information they treat as private for all other purposes should be made available to the police in child pornography cases not because its private character somehow changes, but because in this situation privacy should give way to law enforcement. Whatever one thinks of this as a matter of public policy, the current arrangement suffers from a fatal constitutional defect: s. 8 permits "reasonable" state interferences with privacy interests only if they are "authorized by law". A deal between a group of private corporations and the police, no matter how well-intentioned it may be, is not "law" for *Charter* purposes.

PARTS IV & V: SUBMISSIONS ON COSTS AND REQUEST FOR PERMISSION TO PRESENT ORAL ARGUMENT

20. The CLA does not seek costs and asks that none be awarded against it. The CLA seeks leave to make oral submissions of not longer than 10 minutes.

ALL OF WHICH IS RESPECTFULLY SUBMITTED THIS 24th DAY OF SEPTEMBER, 2013.

JONATHAN DAWE
DAWE & DINEEN
171 John Street, Suite 101
Toronto, Ontario M5T 1X3
Tel: 416-649-5058
Fax: 416-352-7733
E-mail: jdawe@dawedineen.com

JILL R. PRESSER
SCHRECK PRESSERLLP
6 Adelaide Street East, 5th Floor
Toronto, Ontario M5C 1H6
Tel.: (416) 977-6268
Fax: (416) 977-8513
E-mail: presser@schreckpresser.com

COUNSEL FOR THE INTERVENER CRIMINAL LAWYERS' ASSOCIATION OF ONTARIO

---

their request. In this situation different provisions of *PIPEDA* are engaged which expressly authorize this disclosure (see *PIPEDA*, s. 7(3)(d)).

[39] See *Tessling, supra* at ¶64, where the Court (*per* Binnie J.) held that Sopinka J.'s contrary suggestion in *R. v. Plant, supra* should no longer be followed.

PART VI: LIST OF AUTHORITIES

Paragraph

Cases

PART VII: LIST OF RELEVANT STATUTES

Criminal Code, RSC., 1985, c. C-46, s. 487.014	Code criminel, LRC 1985, c C-46
POWER OF PEACE OFFICER	POUVOIR DE L'AGENT DE LA PAIX
487.014 (1)For greater certainty, no production order is necessary for a peace officer or public officer enforcing or administering this or any other Act of Parliament to ask a person to voluntarily provide to the officer documents, data or information that the person is not prohibited by law from disclosing.	**487.014** (1) Il demeure entendu qu'une ordonnance de communication n'est pas nécessaire pour qu'un agent de la paix ou un fonctionnaire public chargé de l'application ou de l'exécution de la présente loi ou de toute autre loi fédérale demande à une personne de lui fournir volontairement des documents, données ou renseignements qu'aucune règle de droit n'interdit à celle-ci de communiquer.
APPLICATION OF SECTION 25	APPLICATION DE L'ARTICLE 25
(2) A person who provides documents, data or information in the circumstances referred to in subsection (1) is deemed to be authorized to do so for the purposes of section 25.	(2) La personne qui fournit des documents, données ou renseignements dans les circonstances visées au paragraphe (1) est, pour l'application de l'article 25, réputée être autorisée par la loi à le faire.

***Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, s. 5(3) and s. 7(3)(*c.1*)(*ii*).**

APPROPRIATE PURPOSES

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

DISCLOSURE WITHOUT KNOWLEDGE OR CONSENT

7 (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;

***Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, c 5, art. 5(3) et 7(3)(*c.1*)(*ii*).**

FINS ACCEPTABLES

5. (3) L'organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.

COMMUNICATION À L'INSU DE L'INTÉRESSÉ ET SANS SON CONSENTEMENT

7 (3) Pour l'application de l'article 4.3 de l'annexe 1 et malgré la note afférente, l'organisation ne peut communiquer de renseignement personnel à l'insu de l'intéressé et sans son consentement que dans les cas suivants :

a) la communication est faite à un avocat — dans la province de Québec, à un avocat ou à un notaire — qui représente l'organisation;

b) elle est faite en vue du recouvrement d'une créance que celle-ci a contre l'intéressé;

c) elle est exigée par assignation, mandat ou ordonnance d'un tribunal, d'une personne ou d'un organisme ayant le pouvoir de contraindre à la production de renseignements ou exigée par des règles de procédure se rapportant à la production de documents;

(*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;

…

(*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;

c.1) elle est faite à une institution gouvernementale — ou à une subdivision d'une telle institution — qui a demandé à obtenir le renseignement en mentionnant la source de l'autorité légitime étayant son droit de l'obtenir et le fait, selon le cas:

(i) qu'elle soupçonne que le renseignement est afférent à la sécurité nationale, à la défense du Canada ou à la conduite des affaires internationales,

(ii) que la communication est demandée aux fins du contrôle d'application du droit canadien, provincial ou étranger, de la tenue d'enquêtes liées à ce contrôle d'application ou de la collecte de renseignements en matière de sécurité en vue de ce contrôle d'application,

(iii) qu'elle est demandée pour l'application du droit canadien ou provincial;

…

d) elle est faite, à l'initiative de l'organisation, à un organisme d'enquête, une institution gouvernementale ou une subdivision d'une telle institution et l'organisation, selon le cas, a des motifs raisonnables de croire que le renseignement est afférent à la violation d'un accord ou à une contravention au droit fédéral, provincial ou étranger qui a été commise ou est en train ou sur le point de l'être ou soupçonne que le renseignement est afférent à la sécurité nationale, à la défense du Canada ou à la conduite des affaires internationale