

Internet and E-Commerce Law in Canada

**Editor-in-Chief: Professor Michael A. Geist, Canada Research Chair in Internet and E-Commerce Law
University of Ottawa, Faculty of Law**

VOLUME 12, NUMBER 5

Cited as (2011-12) 11 I.E.C.L.C.

SEPTEMBER 2011

• E-TRIALS SEEN AS “ESSENTIAL” FOR JUSTICE IN THE FUTURE •

Luigi Benetton

Luigi Benetton Communications

The only one of its kind in Toronto, Courtroom 807 at 393 University Avenue is outfitted for “electronic” trials, a trend many in the legal community see as essential to the evolution of the Canadian justice system.

E-courtrooms aren’t new. Room 807 has been “wired” since 1997, costing \$250,000 when it was first assembled, according to Michael Fernandez, manager of court services for Ontario’s

Superior Court of Justice. “It doesn’t cost any more than a regular courtroom to use,” Fernandez notes.

Room 807 is clearly no ordinary courtroom. For instance, flat-panel monitors sit at each desk, on the judge’s bench and the witness box. During a trial, each screen shows documents displayed by the court registrar as determined by a previously agreed-to road map for the day.

Documents enter the courtroom via physical media, like laptop hard disks and USB memory sticks (a document scanner lets lawyers put hard-copy documents on the screens), since wireless Internet access isn’t yet available and the court doesn’t (yet) allow usage of its servers to store documents. (Should this change, documents could arrive via a court-administered e-filing system — which doesn’t yet exist).

Handling documents electronically remains the main draw for e-courtrooms. “Doing trials electronically cuts court time by at least 25 per cent,” says the Honourable Justice Arthur Gans of Ontario’s Superior Court of Justice.

• In This Issue •	
E-TRIALS SEEN AS ESSENTIAL FOR JUSTICE IN THE FUTURE <i>Luigi Benetton</i>	37
THE INTERNET, CLOUD COMPUTING, AND THE <i>CHARTER</i> RIGHT TO PRIVACY: THE EFFECT OF TERMS OF SERVICE AGREEMENTS ON REASONABLE EXPECTATIONS OF PRIVACY IN CRIMINAL CASES <i>Matthew Nied</i>	40
	

“If we get shorter trials and reduce time worked by judges, court staff and lawyers, it pays for itself quickly,” she adds. “And if 807 is used, there will be more funding to convert more courtrooms.”

[*Editor’s note:* Based in Toronto, Luigi Benetton writes for B2B technology companies as well as for trade and consumer publications. Learn more at www.LuigiBenetton.com]

• THE INTERNET, CLOUD COMPUTING, AND THE *CHARTER* RIGHT TO PRIVACY: THE EFFECT OF TERMS OF SERVICE AGREEMENTS ON REASONABLE EXPECTATIONS OF PRIVACY IN CRIMINAL CASES •

Matthew Nied
Student-at-Law

Introduction

The use of the internet as a tool in the commission of crime has given rise to new search and seizure issues. When individuals use the internet, their personal information may be transmitted to various online service providers, such as social networking websites, email service providers, and internet service providers (“ISPs”). In many cases, online service providers impose terms of service agreements on their users which require them to agree to the disclosure of their personal information to the authorities for the purpose of criminal investigations. Recent decisions indicate that such terms of service agreements are a key factor in assessing the legality of warrantless disclosure in the internet context under s. 8 of the *Canadian Charter of Rights and Freedoms*.¹

These decisions may contribute to an erosion of privacy rights as the internet becomes increasingly central to daily life. Individuals use the internet to perform a variety of personal activities, including writing and receiving correspondence, storing personal files, and developing social networks. However, in order to use these increasingly vital services, individuals must trust their information to online service providers. In doing so, users often unknowingly sub-

ject themselves to non-negotiated terms of service agreements that may limit their privacy expectations. As computing trends fuel a migration of information from personal computers to remote servers controlled by online service providers, more of the public’s information may become exposed to warrantless seizure by the state. This article surveys the law, discusses the effect of terms of service agreements, and considers the privacy implications.

Reasonable Expectations of Privacy on the Internet

Section 8 of the *Charter* provides that “[e]veryone has the right to be secure against unreasonable search or seizure.”² Courts have interpreted this language to require the authorities to obtain prior judicial authorization before intruding on an individual’s reasonable expectation of privacy.³ In the internet context, a reasonable expectation of privacy exists in respect of a “biographical core of personal information” which includes “information which tends to reveal intimate details of lifestyle and personal choices of the individual.”⁴

To challenge the legality of a warrantless search, the accused must first establish that they had a reasonable expectation of privacy.⁵ This

requires the applicant to demonstrate that they had a subjective expectation of privacy and that this expectation was objectively reasonable.⁶ The existence of an objectively reasonable expectation of privacy is determined on the basis of the totality of the circumstances.⁷ Relevant factors include the subject matter of the search, the degree of intrusiveness, whether the information was already in the hands of third parties, and, if so, whether it was subject to an obligation of confidentiality.⁸

The disclosure of user information by online service providers is also governed by the *Personal Information Protection and Electronic Documents Act* [PIPEDA]⁹ and its provincial counterparts.¹⁰ Section 7(3)(c.1) of the PIPEDA permits online service providers to “disclose personal information without the knowledge or consent of the individual” provided that the disclosure is made in response to a request by a government authority that has identified that it is seeking to obtain the information on the basis of “lawful authority”, which courts have generally interpreted as something less than prior judicial authorization.¹¹ However, the PIPEDA does not allow the authorities to avoid seeking prior judicial authorization to obtain disclosure of information that is subject to a reasonable expectation of privacy.¹²

The Effect of Terms of Service Agreements

Several recent decisions have considered the effect of terms of service agreements on reasonable expectations of privacy in the internet context. These decisions have all concerned the issue of whether there is a reasonable expectation of privacy in subscriber information

(name and address) attached to an internet protocol (“IP”) address associated with suspected unlawful activity. These cases reveal that a terms of service agreement is a significant factor to be considered in assessing whether an expectation of privacy is objectively reasonable.

In *R. v. Ward* the police identified an IP address believed to be associated with the sharing of child pornography on the internet.¹³ The police made a warrantless request to the ISP for the subscriber’s name and address pursuant to the PIPEDA. The police obtained the information and relied on it to obtain a warrant to search the accused’s home, which resulted in the discovery of child pornography. The applicant argued that he had a reasonable expectation of privacy in the subscriber information that was critical to obtaining the search warrant, and that the police did not have the authority to receive the disclosure without prior judicial authorization.

The Court concluded in light of the terms of service agreement that the accused did not have a reasonable expectation of privacy in the subscriber information. The agreement provided that the ISP “reserved its right to ... disclose any information necessary to satisfy any laws, regulations, or other governmental request.”¹⁴ It also provided that the accused’s use of the service constituted implied consent for the disclosure. There could be no objectively reasonable expectation of privacy because the online service provider was “entitled to measure its obligation to maintain confidentiality over personal information in accordance with the contractual arrangement with the subscriber.”¹⁵

Courts have reached the same conclusion in numerous cases involving nearly identical facts.¹⁶ Two general observations are worthy of note. First, as in *Ward*, many courts have permitted warrantless disclosure even where the terms of service agreements were broadly phrased and it was not clear from the language that disclosure might occur in the absence of prior judicial authorization. For example, in *R. v. Wilson* the terms of service agreement stated that the ISP could “disclose personal information without knowledge or consent ... to comply with a subpoena, warrant or other court order, or as may be otherwise required by law.”¹⁷ The Court concluded, in the absence of language clearly stating that disclosure could occur in the absence of judicial authorization, that an expectation of privacy could not have been reasonable “by virtue of the contractual terms on which the internet service was provided”.¹⁸ Similarly, in *R. v. Brousseau* the terms of service agreement provided that the ISP would not disclose information other than the subscriber’s “name, address and listed telephone number” if required “pursuant to a legal power.”¹⁹ The Court held that this exclusionary language “disclaim[ed] any suggestion of privacy or confidentiality in the information held by the [ISP].”²⁰

The second noteworthy observation is that courts have held that expectations of privacy may be undermined in circumstances where an accused did not receive formal notice of the permissive disclosure clauses in the terms of service agreement. Courts have found it sufficient that an agreement was published on the online service provider’s website and was available to the accused, even if the accused was unaware of its existence. For example, in *R. v. McNeice* the Court

concluded that although a “lack of formal acknowledgement might be relevant to [an accused’s] subjective expectations of privacy”, it would “not be [objectively] reasonable [for an accused] to not inquire as to the applicable terms of service.”²¹ Similarly, the accused in *R. v. Frieters* could not have a reasonable expectation that his information would remain confidential because the terms of service agreement was “published and available to [the accused] although he did not think to access or investigate the terms under which his internet service was provided.”²²

These decisions appear to be consistent with the conclusion of the Supreme Court of Canada in the recent case of *R. v. Gomboc*.²³ There, the Court considered the effect of a terms of service agreement on an accused’s privacy expectation. The case involved a police investigation which raised suspicions that a marijuana grow operation was located in the accused’s home. The utility that provided electricity to the home cooperated with the police to install a device on the power lines to record the accused’s electricity use. When the device disclosed a pattern of electricity use consistent with a grow operation, the police obtained a search warrant and seized large quantities of marijuana. The accused sought to exclude the evidence on the basis that a warrant had not been obtained prior to installation of the device.

Seven justices of the Court concluded that the expectation of privacy in the electricity consumption information was objectively unreasonable. Central to this conclusion was the existence of a legislative scheme that governed the terms of the relationship between the accused and his utility. The scheme permitted the utility to disclose the accused’s information to the po-

lice for the purposes of investigating an offence, provided that the disclosure was not contrary to any express request made by the consumer.²⁴

The scheme also mandated that the consumer contract include a clause stating that “[i]nformation may be transferred without consent in the case of legal, regulatory or law enforcement requirements.”²⁵ The contract deemed the accused, by using the service, to have accepted this condition.²⁶

The reasons of four justices, written by Justice Deschamps, found that the scheme was one non-determinative factor, albeit an important one, to be considered in the totality of the circumstances.²⁷ That conclusion was partially qualified by the statement that “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 ... there is every reason for proceeding with caution when deciding what independent constitutional effect disclosure clauses ... have on determining a reasonable expectation of privacy.”²⁸ The reasons of three concurring justices, penned by Justice Abella, held that the scheme was determinative to the conclusion that any expectation of privacy was objectively unreasonable.²⁹ This was the case regardless of whether the accused informed himself of the legal parameters of his relationship with the utility.³⁰

Implications for Internet Privacy

The cases support the proposition that an individual’s right to privacy on the internet may be undermined by terms of service agreements that purport to limit privacy expectations. As a result, the issue of whether there is a reasonable expectation of privacy may be determined, in

most cases, by reference to contract.³¹ While this proposition may seem reasonable when considered in cases involving the disclosure of subscriber information, it may cause greater concern when applied to cases involving the disclosure of content information, such as the text of emails, the data contained in online hard drives, and the queries entered into search engines.³² While some online service providers might choose to require the authorities to seek judicial authorization before permitting such serious intrusions,³³ that decision could be theirs alone to make. As the Court noted in *R. v. Cuttell*, these judicial developments may have the effect of shifting the debate about whether disclosure is appropriate “beyond the reach of the courts” and into the hands of the authorities and online service providers.³⁴ As a consequence, the “safeguard of an independent judicial arbiter” may “no longer be available to assess, in advance, whether the individual’s right to privacy should give way to the law enforcement goals of the state.”³⁵

Heightening this concern is a shift in the public’s computing habits. The rise of “cloud computing” — the practice of using the internet to process, manage, and store data on remote network servers — now permits individuals to perform traditionally private activities on the internet. This computing trend is fueling a mass migration of information, once stored on the local hard drives of personal computers, to remote servers in a domain controlled by online service providers.³⁶ Although courts have recognized significant expectations of privacy in respect of information confined to personal computers,³⁷ the same information may now fail to attract similar privacy expectations if uploaded to the

internet and subjected to permissive terms of service agreements.

As a result, the right to privacy on the internet may become dependent on whether the information is stored locally (on an individual's computer), or remotely (by an online service provider). Unfortunately, as online services become less distinguishable from their offline counterparts, average users may have difficulty distinguishing between services that store their personal information remotely rather than locally. Technological advances are now permitting information stored on the internet to appear, to the average user, as though it were stored on their personal computer.³⁸ This may cause users to have an expectation that personal information is on their computers when it is, in fact, stored remotely and is subject to a terms of service agreement that undermines any expectation of privacy.

Such inadvertence or ignorance has generally been irrelevant to the question of whether an individual has an objectively reasonable expectation of privacy. Individuals are presumed to be aware of and understand the terms of service agreements to which they become subject. This is so despite the reality that terms of service agreements are often lengthy, complicated, non-negotiable, and blindly accepted without being read. Many online service providers also reserve the right to modify and amend their terms of service agreements unilaterally at any time.³⁹ In some cases, an individual's acceptance of an agreement may also be based on their use of the service rather than an affirmative signal of their assent to the agreement.⁴⁰ Moreover, because most online service providers have similar agreements, users may have no real alternative

besides forgoing their use of the internet. User consent to terms of service agreements may thus be implicit, uninformed, and partially coerced.

These concerns may support an argument that terms of service agreements should not render an accused's expectation objectively unreasonable where a reasonable person could not be expected to appreciate its impact in the circumstances. This proposition was accepted in a similar context by the dissent in *Gomboc*. Unlike the other justices, McLachlin C.J.C. and Fish J. concluded that the existence of a permissive legislative scheme and terms of service agreement "[did] nothing to render [the accused's] subjective expectation objectively unreasonable" because the reasonable person could not be expected to understand the scheme or be aware of its impact.⁴¹ According to this dissent, a "presumption of awareness" could "not operate to, in effect, narrow the consumer's constitutional rights."⁴²

While this argument seems apposite in the internet context, the result in *Gomboc* may have foreclosed it.⁴³ Three concurring justices held that "attribut[ing] the notional ignorance of an average customer about his or her contractual obligations for purposes of assessing the reasonableness of privacy expectations ... conflates the subjective and objective branches of the privacy inquiry."⁴⁴ The concurring reasons also noted that while an "individual's actual — or imputed knowledge — is undoubtedly relevant when assessing whether there is a subjective expectation of privacy", such "unsubstantiated assumptions about a consumer's state of awareness should not be determinative [when] assessing the objective reasonableness of the expectation."⁴⁵ Such a practice would "collaps[e] the two branches of the

inquiry into a single inquiry into subjectivity.”⁴⁶ Taken to its logical extreme, this view implies that an individual’s subjective expectation of privacy can never be objectively reasonable where there exists a valid contract of adhesion that purports to negate any expectation of privacy.

However, it may remain open for courts to find that an individual’s subjective expectation of privacy is objectively reasonable in the face of a permissive terms of service agreement that is itself unreasonable because its terms are stringent, onerous, or contrary to those that a reasonable person would expect in the circumstances. In the civil context, courts have declined to enforce standard form contracts in circumstances where a party was “unaware of the stringent and onerous provisions”, unless “reasonable measures” were taken to “draw such terms to the attention” of the party.⁴⁷ This reasoning may permit courts to avoid the harsh effect of onerous terms of service agreements on an individual’s expectation of privacy. Similar support for this reasoning may be found in s. 5(3) of the *PIPEDA*, which provides that disclosure may only occur “for purposes that a reasonable person would consider appropriate in the circumstances.”⁴⁸

Alternatively, it might be argued that warrantless disclosure should not be permitted where a disclosure clause is broadly phrased and fails to expressly state that disclosure may occur in the absence of prior judicial authorization. In these circumstances, courts may avoid the effect of a broadly phrased disclosure clause by adopting a narrow interpretation more consistent with an individual’s subjective expectation of privacy. Although courts have yet to take such an approach in cases involving the disclosure of sub-

scriber information, courts may be inclined to do so in cases involving more serious intrusions.

[*Editor’s note*: Matthew Nied, B.Comm. (Alberta), LL.B. (Victoria) clerked at the Supreme Court of British Columbia in 2010-2011. He will article in Vancouver. The views expressed are personal opinions and not those of his employer.]

- ¹ Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11.
- ² *Ibid.*
- ³ *Hunter v. Southam*, [1984] S.C.J. No. 36, [1984] 2 S.C.R. 145 at 159-160 [*Hunter*]; *R. v. Gomboc*, [2010] S.C.J. No. 55, 2010 SCC 55 at para. 17 [*Gomboc*]; *R. v. Plant*, [1993] S.C.J. No. 97, [1993] 3 S.C.R. 281 at 291-293.
- ⁴ *Plant, ibid.* at 293; *Gomboc, ibid.* at paras. 28, 78.
- ⁵ *Gomboc, supra* note 3 at para. 7.
- ⁶ *Ibid.* at para. 18.
- ⁷ *R. v. Edwards*, [1996] S.C.J. No. 11, [1996] 1 S.C.R. 128 at paras. 31, 45; *Gomboc, supra* note 3 at paras. 18, 78, 108.
- ⁸ *Gomboc, supra* note 3 at para. 108.
- ⁹ S.C. 2000, c. 5. The *PIPEDA* attempts to balance the privacy rights of individuals with the need of organizations to collect, use, or disclose that information for purposes that a reasonable person would consider appropriate: *R. v. Cuttell*, [2009] O.J. No. 4053, 2009 ONCJ 471 at para. 38 [*Cuttell*].
- ¹⁰ See e.g. *Personal Information Protection Act*, S.B.C. 2003, c. 63, and *Personal Information Protection Act*, S.A. 2003, c. P-6.5.
- ¹¹ Some courts have noted that the police may have “lawful authority” to receive disclosure of information merely by commencing an investigation: *R. v. Wilson*, [2009] O.J. No. 1067 (S.C.J.) [*Wilson*]; *R. v. Vasic*, [2009] O.J. No. 685, 185 C.R.R. (2d) 286 (S.C.J.) [*Vasic*]; *R. v. Kwok*, [2008] O.J. No. 2414 at para. 32 (C.J.) [*Kwok*]; *R. v. Brousseau*, [2010] O.J. No. 5793, 2010 ONSC 6753 at para. 43 [*Brousseau*]. However, compare with *C.(S.), Re*, [2006] O.J. No. 3754, 2006 ONCJ 343 where the Court found that the mere existence of a criminal investigation was not enough to constitute “lawful authority.”
- ¹² *Cuttell, supra* note 9 at paras. 45, 48; *R. v. Ward*, [2008] O.J. No. 3116, 2008 ONCJ 355 at para. 57 [*Ward*]; *Kwok, supra* note 11 at paras. 34-35;

R. v. Trapp, [2009] S.J. No. 32, 2009 SKPC 5 at para. 11 [*Trapp*].

¹³ *Ward*, *supra* note 12.

¹⁴ *Ibid.* at para. 46.

¹⁵ *Ibid.* at paras. 40, 67-68.

¹⁶ *Cuttell*, *supra* note 9 at paras. 30-33, 59; *Wilson*, *supra* note 11 at paras. 35, 43; *Vasic*, *supra* note 11; *Trapp*, *supra* note 12 at para. 12; *R. v. Verge*, [2009] O.J. No. 6300 (C.J.) at para. 41; *R. v. Friers*, [2008] O.J. No. 5646, 2008 ONCJ 740 at paras. 25, 30 [*Friers*]; *Brousseau*, *supra* note 11 at paras. 46, 50; *R. v. McNeice*, [2010] B.C.J. No. 2131, 2010 BCSC 1544 at para. 46 [*McNeice*]; *R. v. Spencer*, [2009] S.J. No. 798, 2009 SKQB 341 at para. 19.

¹⁷ *Wilson*, *supra* note 11 at para. 35.

¹⁸ *Ibid.* at para. 43.

¹⁹ *Brousseau*, *supra* note 11 at para. 28.

²⁰ *Ibid.* at para. 30.

²¹ *McNeice*, *supra* note 16 at para. 46; *Vasic*, *supra* note 11 at paras. 55-56.

²² *Friers*, *supra* note 16 at para. 21.

²³ *Gomboc*, *supra* note 3.

²⁴ *Ibid.* at paras. 31, 84.

²⁵ *R. v. Gomboc*, [2009] A.J. No. 892, 2009 ABCA 276 at paras. 88, 92.

²⁶ *Ibid.* at para. 89.

²⁷ *Gomboc*, *supra* note 3 at para. 32.

²⁸ *Ibid.* at para. 33.

²⁹ *Ibid.* at paras. 58, 82, 95.

³⁰ *Ibid.* at para. 57.

³¹ *Cuttell*, *supra* note 9 at para. 79. See also *R. v. Ballendine*, [2011] B.C.J. No. 838, 2011 BCCA 221 at para. 78, where the Court cited *Gomboc*, *supra* note 3 and stated that “the terms of [a] contract can be important in making a determination as to whether a customer has a reasonable expectation of privacy in ... customer-account information disclosed” in the internet context.

³² However, it should be noted that subscriber information may be worthy of greater privacy protection than content information even though it appears, on its face, to be less revealing. Subscriber information may permit the state to connect the identity of an individual to their online activities. See Daphne Gilbert, Ian R. Kerr & Jena McGill, “The Medium and the Message: Personal Privacy and the Forced Marriage of Police and Telecommunications Providers” 51 *Crim. L.Q.* 469 at 488.

³³ See e.g. *Ward*, *supra* note 12 at paras. 47-51. See also *Kwok*, *supra* note 11 at para. 12.

³⁴ See e.g. *Cuttell*, *supra* note 9 at para. 80.

³⁵ *Ibid.*

³⁶ The global cloud computing market is expected to increase from \$37.8 billion in 2010 to \$121.1 billion in 2015, at a compound annual growth rate of 26.2 per cent: “Cloud Computing Market — Global Forecast (2010 -2015)” October 2010, online: <<http://www.marketsandmarkets.com/Market-Reports/cloud-computing-234.html>>.

³⁷ *R. v. Morelli*, [2010] S.C.J. No. 8, 2010 SCC 8 at para. 105.

³⁸ For example, Google introduced a new web browser in 2008 which permits users to create a desktop version of any online application which operates exactly like a regular desktop program. This feature seeks to completely integrate online applications within the desktop. As one commentator noted, the development significantly “blurs the line between online and offline software.” See David Pogue, “Serious Potential in Google’s Browser”, *N.Y. Times*, Sept. 3, 2008, at C1. Google has also announced the imminent release of an operating system based entirely on cloud computing technology: Paul Boutin, “Google’s Chrome OS: Putting Everything in the Browser Window”, *N.Y. Times*, January 18, 2011, online: <<http://gadgetwise.blogs.nytimes.com/2011/01/18/googles-chrome-os-putting-everything-in-the-browser-window/>>.

³⁹ See e.g. *McNeice*, *supra* note 16.

⁴⁰ *Vasic*, *supra* note 11 at para. 46.

⁴¹ *Gomboc*, *supra* note 3 at paras. 139, 142.

⁴² *Ibid.* at para. 139.

⁴³ *Ibid.* at para. 32.

⁴⁴ *Ibid.* at para. 93.

⁴⁵ *Ibid.*

⁴⁶ *Ibid.*

⁴⁷ *Tilden Rent-a-Car Co. v. Clendenning*, [1978] O.J. No. 3260, 83 D.L.R. (3d) 400 (C.A.) at para. 32. See also *Interfoto Picture Library Ltd. v. Stiletto Visual Programmes Ltd.*, [1989] 1 Q.B. 433 (C.A.).

⁴⁸ Section 5(3), *PIPEDA*, *supra* note 9.

ELECTRONIC VERSION AVAILABLE

A PDF version of your print subscription is available for an additional charge.

**A PDF file of each issue will be e-mailed directly to you 12 times per year,
for internal distribution only.**

INVITATION TO OUR READERS

**Do you have an article that you think would be appropriate for
Internet and E-Commerce Law in Canada and that you would like to submit?**

AND/OR

**Do you have any suggestions for topics you would like to see featured in future issues
of *Internet and E-Commerce Law in Canada*?**

**If so, please feel free to contact Michael A. Geist
@mgeist@uottawa.ca
OR
ieclc@lexisnexis.ca**