17 No. 9 J. Internet L. 3

Journal of Internet Law
March, 2014

Matthew Nied, Shawn Erker [a1]

CLICKING AWAY PRIVACY: EMAIL AND THE TORT OF INTRUSION UPON SECLUSION

Email doesn't need postage. Today, many service providers offer email accounts for free and monetize them through advertising. For example, every email sent to or from an account with "Gmail," Google's popular email service, is an advertising opportunity for Google. This is because Google, or, rather, its computer algorithms, "reads" each email as it arrives or departs, scanning for keywords that will trigger corresponding advertisements. As a result, an email that mentions photography may, when viewed by the recipient, display an advertisement for cameras. [1]

In October 2012, Wayne Plimmer filed a class-action lawsuit against Google in British Columbia. [2] Mr. Plimmer, a non-Gmail user, claims that Googe has been "reading" emails that he has sent to Gmail users, that he has never consented to Google's use of his private emails for advertising purposes, and that Google is liable for damages for invading his privacy. [3] The claim alleges invasion of privacy under both the common law and the British Columbia *Privacy Act*. [4] Gmail had more than 425 million active users in or around the time of the filing of the claim. [5]

More than 120 years before, on a day in 1890, Samuel D. Warren, a Boston attorney, felt a similar frustration with his own privacy interests. He and his wife had hosted a series of elite social events, including a wedding for their daughter, which the Boston newspapers had covered in highly personal and embarrassing detail. [6] Exasperated, Warren approached his former law partner, Louis D. Brandeis, with the desire of finding some legal remedy for this constant invasion of privacy, one that would protect his right to be "left alone."

Later that year, Warren and Brandeis published "The Right to Privacy" in the *Harvard Law Review*. [7] It called for common-law protection for, among other items falling within the penumbra of privacy, the use of private letters by an unintended third-party recipient. [8]

In 1939, this proposed right to privacy was incorporated into the *Restatement of Torts*, and by 1960 it was adopted in 26 states and the District of Columbia. [9] In 1977, the *Restatement (Second) of Torts* provided as an example of such a tort an "investigation or examination into [one's] private concerns, *as by opening his private and personal mail*." [10] Throughout the 20th century, it was taken as established that reading someone else's mail would satisfy the elements of this tort.

By 2001, all but two US states had recognized some form of a right to privacy, [11] and today the concept has begun to make its way into Canadian law. [12] Yet, as the tort gains wider acceptance, its scope is called into question when considered in the new context of Internet communications. Although Warren and Brandeis bristled at the thought of third parties intercepting private mail, the facts of *Plimmer v. Google* have been described by one academic as an "are-you-kidding-me" lawsuit. [13]

This article explores why the act of intercepting and reading another's mail-- an act that was initially viewed as an obvious *example* of an invasion of privacy--could today be viewed by some as an obvious nonstarter. This article first compares the common-law invasion-of-privacy regime in Ontario with the statutory regime in British Columbia. The regimes in these provinces are among the most developed of the Canadian invasion-of-privacy regimes and generally are representative of the common law and statutory regimes in other Canadian jurisdictions. It is suggested that, in practice, the analysis applicable ***4** to the tort of intrusion upon seclusion, as a subset of invasion of privacy, is similar under both the common law and statutory regimes.

Next, the article surveys US jurisprudence, which has informed the development of Canadian law, and shows why voluntary disclosure of information to a third party may have different implications under the Canadian common law regime than it does in the United States. Finally, the article explores the impact of consent under the common law and statutory regimes, and briefly considers the potential implications for a case such as *Plimmer*.

INVASION OF PRIVACY IN CANADA

JONES V. TSIGE AND THE COMMON LAW TORT IN ONTARIO

In *Jones v. Tsige*, the Ontario Court of Appeal explicitly recognized a common law tort of invasion of privacy. The case arose after Tsige, an employee at Jones' bank, accessed Jones' banking records at least 174 times. [14] Tsige was in a relationship with Jones' former husband and claimed to be accessing the information to confirm aspects of a financial dispute between Jones and her former husband. [15] Tsige acknowledged that this was contrary to the bank's policies and apologized for her actions. [16] Justice Sharpe found that the defendant's conduct was "deliberate, prolonged and shocking." [17] He stated that, in his view, "the law of [Ontario] would be sadly deficient if we were to send Jones away without a legal remedy." [18] In searching for such a remedy, Justice Sharpe pointed to the description of the US tort of "invasion of privacy" by academic William Prosser. [19] Prosser described four different manifestations of the tort of invasion of privacy: (1) intrusion upon seclusion; (2) public disclosure of private facts; (3) publicity that places the plaintiff in a false light; and (4) appropriation, for the defendant's advantage, of the plaintiff's name or likeness. [20] The relevant form for both the Court in *Jones*, as well as for the purposes of this article, is the tort of intrusion upon seclusion, which, for convenience, we will call the "tort of Intrusion."

After reviewing the history of the tort of Intrusion in the United States, Justice Sharpe found it appropriate for the Court to confirm the existence of such a cause of action in Ontario. [21]

In defining the scope of the tort of Intrusion, Justice Sharpe "essentially adopt[ed]" [22] the definition given in the *Restatement (Second) of Torts* (2010): "One who intentionally intrudes, physically or otherwise, upon the seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the invasion would be highly offensive to a reasonable person." [23]

THE DIFFERENT (OR SIMILAR) TORT REGIMES IN BRITISH COLUMBIA AND ONTARIO

Unlike Ontario, British Columbia courts have to date not recognized a common law tort of invasion of privacy. In fact, since the decision in *Jones*, British Columbia courts have, on at least two occasions, stood firm in asserting that such a common law cause of action does not exist in British Columbia. [24] While BC courts not given an explicit explanation for why the tort does not exist in the province, besides pointing to precedent predating *Jones*, [25] an obvious explanation is that the tort would be largely redundant within the province because of the existence of an equivalent statutory remedy under British Columbia's *Privacy Act*. [26]

In *Nesbitt v. Neufeld*, [27] Justice Crawford described the language of the *Privacy Act* as "codif[ying] the tort of invasion of privacy," [28] suggesting that courts in British Columbia are dismissing claims for invasion of privacy under the common law not because of a jurisprudential opposition to its existence, but because the legislature has superseded it.

In general, the provincial privacy statutes establish a limited cause of action whereby liability will be found only if the defendant acts willfully and without a claim of right. [29] Moreover, the nature and degree of the plaintiff's privacy entitlement is circumscribed by what is "reasonable in the circumstances." The legislation does not provide precise guidance as to what constitutes an invasion of privacy. [30]

Interestingly, the lack of guidance provided in the provincial legislation has in some cases led courts to an analysis much like that under the common law in *Jones*. For example, in *Nesbitt v. Neufeld*, the plaintiff was suing for, *inter alia*, an intrusion upon her ***5** privacy. [31] During a custody battle, the defendant sent the content of private emails between the plaintiff and a friend to third parties. [32] The British Columbia Supreme Court found that the plaintiff had a "reasonable expectation that her personal information and private correspondence [would] not be emailed ... to third parties ... without her knowledge and consent," [33] and accordingly found the defendant liable for both breach of privacy and defamation. [34] In considering the claim, the Court looked first to the language of the British Columbia *Privacy Act*, but then supplemented the language of the statute by looking to Prosser's "classification of interests protected by the law of privacy as developed in the United States." [35] This was the same seminal article the Court in *Jones* looked at as a foundation for the Ontario common law tort. [36]

Despite the torts' divergent origins in British Columbia and Ontario, both jurisdictions have looked and, in all likelihood, will continue to look to the US experience to flesh out the parameters of the tort in novel circumstances.

THE US TEST FOR INTRUSION UPON SECLUSION

In the United States, the tort of Intrusion has the following elements:

1. There was an unauthorized intrusion;

2. The intrusion was highly offensive to the reasonable person;

3. The matter intruded upon was private; and

4. The intrusion caused anguish and suffering. [37]

The cases often turn on the presence or absence of the third element. In order to establish that a matter was private in satisfaction of the third element, the claimant must show that he or she had a "reasonable expectation of privacy" in respect of the matter. The test for determining whether a claimant had a reasonable expectation of privacy is the same as

the test that applies to the Fourth Amendment of the Constitution. [38] The first step is demonstrating an actual subjective expectation of privacy, and the second step asks if that expectation is objectively reasonable. [39]

In *Smith v. Maryland*, [40] one of the leading US Supreme Court cases on reasonable expectations of privacy, an accused attempted to have evidence of his phone records thrown out of his criminal trial. The Court declined to do so, finding that the accused did not have a reasonable expectation of privacy in his phone records. [41] The Court reasoned that because the accused had to communicate the phone numbers he was calling to the telephone service provider in order to make the calls in the first place, he was voluntarily providing the data in question to a third party and therefore waiving any privacy interest in it. [42]

This case led to the development of a legal doctrine commonly known as "risk analysis." This doctrine holds that a person does not have a reasonable expectation of privacy in information if the person took the risk in providing the information to a third party because that third party could, in turn, provide the information to another person. [43]

The US risk-analysis cases suggest that while people may have some expectation of privacy in their received mail--based on the reasonable expectation that an intruder would not open their mailbox and read its contents--a sender of mail, by voluntarily sending the mail to a third party, has no equivalent reasonable expectation of privacy. [44]

In contrast to the United States, the Supreme Court of Canada has decidedly rejected the US line of risk-analysis cases. [45] This means that while Canadian courts may begin their analysis into the tort of Intrusion by looking to US precedent, it is likely that courts will turn to Canadian constitutional jurisprudence to determine whether there is a reasonable expectation of privacy.

REASONABLE EXPECTATION OF PRIVACY IN CANADA

The *Charter* provides protection from state interference, as does the US Constitution. In particular, Section 8 of the *Charter* provides that "[e]veryone has the right to be secure against unreasonable search or seizure." [46] Courts have interpreted this language to require government authorities to obtain prior judicial authorization, typically in the form of a warrant, before intruding on an individual's reasonable expectation of privacy. [47] Courts have recognized that a reasonable expectation of privacy applies to, among other things, a "biographical core of personal information" that includes "information which tends ***6** to reveal intimate details of lifestyle and personal choices of the individual." [48]

While the *Charter* does not apply to common law disputes between private individuals, courts have acted on several occasions to develop the common law in a manner consistent with *Charter* values. [49] Notably, the *Jones* court expressly considered *Charter* jurisprudence before concluding that "[t]he explicit recognition of a right to privacy as underlying specific Charter rights and freedoms" supported "the recognition of a civil action for damages for intrusion upon the plaintiff's seclusion." [50] The *Jones* court also observed that the "[t]he right to informational privacy [recognized in *Charter* jurisprudence] closely tracks the same interest that would be protected by a cause of action for intrusion upon seclusion." [51]

Charter jurisprudence also may inform developments in the statutory privacy regime. In *Bigstone v. St. Pierre*, [52] the Saskatchewan Court of Appeal analyzed the scope of the Saskatchewan *Privacy Act*, which is largely equivalent to the British Columbia *Privacy Act*. In doing so, Justice Ottenbreit said, "apart from the Act, *the development of the concept and categories of privacy interests has been largely driven by Charter cases*. The generally accepted categories include personal, territorial and *informational privacy*." [53]

To establish a reasonable expectation of privacy, a *Charter* applicant must demonstrate that the applicant had a subjective expectation of privacy and that this expectation was objectively reasonable. [54] The existence of an objectively reasonable expectation of privacy is determined on the basis of the totality of the circumstances. [55] Relevant factors include the subject matter, 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. [56] A reasonable expectation of privacy would therefore be impacted by disclosure to a third-party, but in contrast to the US risk-analysis case law, would not necessarily be waived by it. [57]

CONSENT, TERMS OF SERVICE AGREEMENTS, AND THEIR IMPACT ON REASONABLE EXPECTATIONS OF PRIVACY

The presence or absence of consent to an invasion of privacy can be an important factor in the analysis under the common law and statutory privacy regimes. In respect to the statutory regime, Section 2(2)(a) of the British Columbia *Privacy Act* deems it to not be a violation of privacy if the act or conduct was "consented to by some person entitled to consent." [58] In respect to the common law regime, a party's consent to an invasion of privacy may undermine the party's ability to demonstrate a reasonable expectation of privacy.

The only case dealing with the issue of consent in the context of the British Columbia *Privacy Act* is *Hollinsworth v. BCTV*. [59] In that case, the plaintiff had consented to the videotaping of a tunnel graft surgery procedure to disguise his baldness and to the use of that video for medical instructional purposes only. Seven years later, the parties that conducted and videotaped the original procedure provided the videotape, which clearly showed the plaintiff's face, to a broadcasting station, which subsequently aired it. The plaintiff sued the broadcasting station, among others, for an invasion of privacy in breach of the *Privacy Act*.

The trial court referred to Section 2(2)(a) of the *Privacy Act* and determined that although the parties who gave the tape to the broadcasting station were liable to the plaintiff, the broadcasting station was not. In reaching that conclusion, the trial judge noted that the parties that had conducted and videotaped the original procedure gave the broadcasting station consent to use the tape and assured them that the plaintiff had consented. The case at the trial level was dismissed as against the broadcasting station on that basis. [60]

When applied by analogy to the context of email, the decision may support an argument that if Party A sends an email to Party B, and Party B consents to the disclosure of the email to Party C, then in certain circumstances Party C will be protected from a claim by Party A, although Party A may still have a claim against Party B.

Consent is often a significant consideration in the context of Internet communications. When individuals use the Internet, their personal data is transmitted to various service providers. Those service providers often impose "terms of service agreements" which provide that personal data may be disclosed or used in certain circumstances. These contractual "consent forms" usually are not read by even the most discerning users. [61]

***7** Recent decisions under Section 8 of the *Charter* indicate that an individual's reasonable expectation of privacy may be undermined by such terms of service agreements. [62] As the law develops, courts may apply the reasoning in these decisions to lawsuits involving breaches of privacy.

The leading decision on the subject was issued by the Ontario Court of Appeal a few months after *Jones*. In *R. v. Ward*, [63] the accused was charged with possessing and accessing child pornography. During the investigation, the police, without a search warrant, obtained information from the accused's Internet service provider (ISP) that identified the accused as

the person who had viewed a particular pornographic Web site at a particular time. The accused argued that he had a reasonable expectation of privacy in the information, and that the police did not have the authority to receive the disclosure without a warrant.

The terms of service agreement between the accused and the ISP provided, among other things, that the ISP could disclose the accused's subscriber information to the police in connection with criminal investigations. It also provided that customers, by subscribing to the service, automatically consented to the collection, use, and disclosure of their personal information as described in the service agreement, unless the customer specifically withdrew that consent by completing an "opt-out form." There was no evidence that the accused had ""opted out". [64]

The trial 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." [65] 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." [66]

On appeal, the Court observed that the terms of service agreement was "a classic contract of adhesion" in which the ISP "unilaterally set the terms of the service agreement and related documents." [67] The Court ultimately concluded that the accused did not have a reasonable expectation of privacy, and that the contractual provisions tended to reinforce that conclusion. [68]

However, the Court observed that "willing disclosure to third parties is not determinative of the existence of a legitimate privacy claim under s. 8" [69] and emphasized that the result in the case was based on specific circumstances and was "not intended to suggest that disclosure of customer information by an ISP can never infringe the customer's reasonable expectation of privacy." [70]

Courts have reached similar conclusions in numerous cases involving nearly identical facts. [71] Significantly, courts have held that terms of service agreements can undermine privacy expectations even when an individual did not receive formal notice of the permissive disclosure clauses in the agreement. Courts have found it sufficient that an agreement was published on the online service provider's Web site and was available to the individual, even if the individual was unaware of its existence. [72]

One might be tempted to argue that consent should not be considered effective unless it is fully informed and express. However, in general, a user's ignorance of a terms of service agreement is irrelevant to the question of whether the user has an objectively reasonable expectation of privacy. Instead, users have been presumed to be aware of and understand the terms of service agreements to which they become subject.

This may give rise to further concern when service providers reserve the right to modify and amend their terms of service agreements unilaterally at any time, [73] or when an individual's acceptance of an agreement is based on the individual's use of the service rather than an affirmative signal of his or her assent to the agreement. [74] In addition, because most online service providers have similar agreements, users may have no real alternative. Accordingly, user consent to terms of service agreements may be implicit, uninformed, and partially coerced.

The issue is highlighted by the recent decision of the Supreme Court of Canada in *R. v. Gomboc*. The case involved a police investigation that raised suspicions that the accused's home contained a marijuana grow operation. 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, ***8** 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 police for the purposes of investigating an offense, provided that the disclosure was not contrary to any express request made by the consumer. [75] 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." [76] The contract deemed the accused, by using the service, to have accepted this condition. [77]

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. [78] 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." [79]

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. [80] This was the case regardless of whether the accused informed himself of the legal parameters of his relationship with the utility. [81]

In particular, the 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." [82] 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." [83]

Despite the impact of these authorities, 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. [84] This reasoning may permit courts assessing privacy breaches in the civil context to avoid the harsh effect of onerous terms of service agreements on an individual's expectation of privacy.

CONCLUSION

Having surveyed the burgeoning invasion-of-privacy regimes in Canada and considered the manner in which they might evolve, we return to briefly consider how the law could apply to a case involving the tort of Intrusion in the context of email.

As it turns out, the answer may well depend on which of the invasion-of-privacy regimes apply. We have shown how, despite divergent origins, courts in British Columbia and Ontario have developed the tort along parallel, and largely equivalent, paths--both using the same US jurisprudence to fill in the scope of just what "invasion of privacy" might entail. However, there is potential for divergence on the issue of consent.

One key element of *Plimmer* is that the plaintiff had no contractual relationship with Google. However, the recipients of the plaintiff's emails did have such a relationship, and those recipients had, through that relationship, consented to Google's act of "reading" the emails. [85]

Under the common law and statutory regimes, it is clear that Party A cannot have a claim against Party B based on an email received by Party A from Party C if Party A consented through a terms of service agreement to disclosure of that email to Party B.

***9** However, because Canadian courts have rejected the "risk analysis" doctrine prevalent in US law, it seems likely that the Canadian common law regime will not hold Party C to have waived his or her reasonable expectation of privacy in the email as against Party B merely because Party C sent the email to Party A, who in turn consented to disclose it to Party B. Party C could conceivably still claim that he or she held a reasonable expectation of privacy in the email if he or she actually held a subjective expectation of privacy and that expectation was objectively reasonable. A personal email sent from a doctor to a patient, or even a solicitor to his or her client, might contain private, possibly privileged information that the sending party has every expectation will remain private. A party not privy to the email provider's terms of service may have no reason to suspect that such privacy is imperiled.

The result may be different under the statutory regime. Under the British Columbia *Privacy Act*, a defendant is protected from a claim if the defendant obtained consent from a person "entitled to consent." While there is limited precedent available on this point, one might rely on this language to argue that Party A's consent to disclose the email to Party B provides Party B with a defense against Party C in appropriate circumstances, although Party C might still have a claim against Party A. This language, as well as similar language in comparable legislation in other Canadian jurisdictions, may well send the statutory regime along a different development path as the modern law of privacy develops.

Footnotes

a1 ***Matthew Nied*** *practices business litigation and dispute resolution at Stikeman Elliott in Vancouver, Canada.* ***Shawn Erker*** *is a J.D. student at the University of British Columbia as well as the Editorin-Chief--Editorial of the UBC Law Review.*

1 *See* Martha Mendoza, "Google says it has a right to scan your email," Associated Press, online: CTV News, *http:// www.ctvnews.ca/sci-tech/google-says-it-has-a-right-to-scan-youremail1.1441131.*

2 *See* Notice of Civil Claim "Plimmer v. Google," online: *Sribd http:// www.scribd.com/doc/109372535/Plimmer-v-Google* [Plimmer].

3 *See* Plimmer, *supra* n.2 at Part 1, paras. 6-7.

4 *Id.* at Part 2, paras. 1(b)(i)-(ii).

5 Dante D'Orazio, "Gmail now has 425 million active users," The Verge, online: *http://www.theverge.com/2012/6/28/3123643/ gmail425-million-total-users.*

6 This account is taken from William L. Prosser, "Privacy," 48:3 *Cal L Rev* 383 at 383-384 (1960). It has been suggested by some authors that this may be apocryphal, and the actual impetus behind the article is contested. *See* Amy Gajda, "What if Samuel D. Warren Hadn't Married a Senator's Daughter?: Uncovering the Press Coverage that Led to the Right to Privacy," 1 *Michigan State Law Review* 134 (2008).

7 Samuel D. Warren & Louis D. Brandeis, "The Right to Privacy," 4:5 *Harvard L Rev* 193 (1890).

8 *Id.* at 201, 211-212 (Warren and Brandeis felt that the traditional reasons given for granting an injunction against the publication of such letters, that of breach of confidence, contract, or trust, was an unsound explanation for what was, at its heart, a right to privacy in mail against the whole world).

9 *See* Prosser, *supra* n.6 at 386-387.

10 Restatement (Second) of Torts § 652B, cmt b (1977) [emphasis added].

11 *See* Gregg M. Fishbein & Ellingstad, "Internet Privacy: Does the Use of 'Cookies' Give Rise to a Private Cause of Action for Invasion of Privacy in Minnesota?" 27 *Wm Mitchell L Rev* 1609 at 1611 (2000).

12 *See* Jones v. Tsige, 2012 ONCA 32 *rev'g* 2011 ONSC 1475 [Jones]; Trout Point Lodge Ltd v. Handshoe, 2012 NSSC 245.

13 Gillian Shaw, "G-mail lawsuit an 'are-you-kidding-me' type case, says U.S. academic," *Vancouver Sun* (October 7, 2012) (*quoting* Eric Goldman of Santa Clara University School of Law).

14 *Jones* at para. 4.

15 *Id.* at paras. 4-5.

16 *Id.* at para. 6.

17 *Id.* at para. 69.

18 *Id.*

19 *Id.* at para. 19.

20 *Id.* at para. 18.

21 *Id.* at para. 65.

22 *Id.* at para. 70.

23 *Id. citing* Restatment (Second) of Torts § 652B (1977).

24 *See* Ari v. Ins. Corp. of British Columbia 2013 BCSC 1308 at para. 63; Demcak v. Vo, 2013 BCSC 899 at para. 64. In contrast, after the common law tort was confirmed in Ontario, the Supreme Court of Nova Scotia acknowledged that the commonlaw tort does exist in Nova Scotia. *See Trout Point Lodge* at para. 55.

25 *See Ari* at para. 63 *citing* Hung v. Gardner, 2002 BCSC 1234.

26 RSBC 1996, c 373. Three other Canadian provinces have similar legislation. *See* Privacy Act, RSM 1987 c P125 (Manitoba); The Privacy Act, RSS 1978, c P-24 (Saskatchewan); Privacy Act, RSN 1990, c P-22 (Newfoundland). In Quebec, the right to privacy is explicitly protected both by Articles 3 and 35-37 of the Civil Code of Quebec and by Section 5 of the Charter of Human Rights and Freedoms, RSQ, c C-12. *See also Jones* at para. 53.

27 Nesbitt v. Neufeld, 2010 BCSC 1605.

28 *Id.* at para. 87 [emphasis added].

29 Willfulness is not a requirement in Manitoba. *Jones* n.12 at para. 52.

30 *Jones* n.12 at para. 54.

31 *Id.* at para. 2.

32 *Id.* at paras. 22 and 93. The defendant had obtained an old computer belonging to the plaintiff and had removed the personal emails from the hard drive before distributing them to third parties (*Id.* at para. 11).

33 *Id.* at para. 92.

34 *Id.* at para. 104.

35 *Id.* at para. 88.

36 *Jones* at para. 19.

37 *Id.* at paras. 55-56.

38 *See* David A. Elder, The Law of Privacy (New York: Clark Boardman Callaghan, 1991) at s 2:6, p 41. *See also* Jay P. Kesan, Carol M. Hayes & Masooda N. Bashir, "Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency," 70 *Wash & Lee L Rev* 341 at 408-13 (2013). The Constitutional protection of privacy was greatly expanded in this regard, beyond physical intrusions to a more general protection of private information, by the Supreme Court of the United States in *Katz v. United States*, 389 US 347 (1967) at 351 (the Constitution protects "people, not places"). *See also* Elder, *supra* n.38 at s 2:6, p 41. This has included protection for personal mail, *see, e.g.*, Vernars v. Young, 529 F2d 966, 968 (CA3 Pa 1976) ("[j]ust as private individuals have a right to expect that their telephonic communications will not be monitored, they also have a reasonable expectation that their personal mail will not be opened and read by unauthorized persons").

39 *Jones* at para. 59.

40 Smith v. Maryland, 442 US 735 (1979).

41 *Id.* at 745.

42 *Id.* at 743-744.

43 *See* United States v. Miller, 425 US 435, 442-443, 96 S Ct 1619. This has been recently questioned by Judge Sotomayor in United States v. Jones, 132 S Ct 945; 181 L Ed 2d 911, where she said "[i]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."

44 This actually is the argument made by Google in a recent class action filing in California with facts analogous to those in Plimmer v. Google; *see* In re Google Inc. Gmail Litigation, 13-md-02430, US District Court, Northern District of California, Notice of Motion and Motion to Dismiss, online: Word to the Wise, *http://blog.wordtothewise.com/wp-content/uploads/2013/08/gov. uscourts.cand_.264869.44.0.pdf* [*In re Google*]. Google points to *Smith v. Maryland* as authority for the proposition that there is no reasonable expectation of privacy in emails sent to Gmail users (*Id.* at 19). Google claims that, since they are a service provider, they should be treated like a phone company--a necessary third party that the plaintiffs have voluntarily provided their information to, waiving all privacy interests in the process (*Id.*).
In the United States, much of this area of the common law has been superseded by wire-tapping legislation. Although the California lawsuit deals with such a statute, the arguments put forward in defense of Google are equivalent to those used in the Constitutional and common law tort settings. At the time of this writing, the California Court has rejected Google's application to strike the plaintiff's claim; Google is attempting to appeal the decision. *See* Linda Sandler, "Google Seeks to Appeal U.S. Judge's Gmail Wiretap Ruling," online: *Bloomberg http://www.bloomberg.com/news/2013-10-10/google-seeks-to-appeal-u-s-judge-sgmailwiretap-ruling.html.*
However, some US courts *have* found the existence of a reasonable expectation of privacy in emails. For example, in the case of *United States v. Warshak*, 631 F 3d 266 (6th Cir 2010), the federal circuit court determined that the accused, whose emails were seized from an ISP by government officials, held a reasonable expectation of privacy in his emails (*Id.* at 274). This was true despite the fact that his service provider had the contractual authority to access his emails "as necessary to protect the service" (*Id.* at 289)--essentially, he had taken the risk that they would indeed access the emails if ordered by government, but the Court likened it to the knowledge that, just because a person may know it's possible for the operator to listen to a private conversation, doesn't mean they don't still have a reasonable expectation of privacy in the conversation (*Id.* at 287-288).

This raises the question of whether sending an email can really be compared to the facts of *Smith v. Maryland*. While the actual digits of the phone number were required by the phone company to complete the call, the content of an email, outside of the data relating to destination, is irrelevant to the actual service being provided by an email provider. Even the monetization of the service through advertisements does not require the personal data acquired through emails, although its effectiveness would be fettered.

45 *See* R v. Duarte, [1990] 1 SCR 30 at 48; 71 OR (2d) 575.

46 Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (U.K.), 1982, c. 11.

47 *See* Hunter v. Southam, [1984] SCJ No. 36, [1984] 2 SCR 145 at 159-160 [Hunter]; R v. Gomboc, [2010] SCJ No. 55, 2010 SCC 55 at para. 17 [Gomboc]; R v. Plant, [1993] SCJ No. 97, [1993] 3 SCR 281 at 291-293 [Plant].

48 *Plant* at 293; *Gomboc* at paras. 28, 78.

49 *See* Hill v. Church of Scientology, [1995] 2 SCR 1130 at para. 85; R v. Salituro, [1991] 2 SCR 654 at 675.

50 *Jones* at paras. 39-46.

51 *Id.* at para. 66.

52 Bigstone v. St. Pierre, 2011 SKCA 34 [*Bigstone*].

53 *Id.* at para. 20 [emphasis added]. However, it appears that *Charter* case law on reasonable expectations of privacy cannot, alone, describe the full scope of potential liability under the tort of Intrusion. In *Bigstone*, the Saskatchewan Court of Appeal said the following:
The *Act* does not appear to be designed like ss 7 and 8 of the *Charter*, as a shield to limit state infringement of privacy, but rather a sword to allow compensation of infringement of privacy. This suggests that the privacy that the *Act* protects may be more extensive, and different in some respects, than privacy under the *Charter*. The analytical approach to whether an expectation of privacy exists and is breached in a particular case may be different than the approach in *Charter* cases.
Bigstone at para. 21.

54 *Gomboc* at para. 18.

55 R v. Edwards, [1996] SCJ No. 11, [1996] 1 SCR 128 at paras. 31, 45; *Gomboc* at paras. 18, 78, and 108.

56 *Gomboc* at para. 108.

57 Confidentiality would also raise issues in the context of service providers reading emails: Solicitor--client privilege would attach to any email communication, yet Gmail, *e.g.*, would "read" these emails the same as any other.

58 Privacy Act, s 2(2)(a).

59 Hollinsworth v. BCTV, [1996] BCJ No. 2638; 34 CCLT (2d) 95.

60 *Id.* at para. 21. On appeal, Justice Lambert did not consider Section 2(2)(a), but instead disposed of the claim by determining that, because the television program was under the impression that the plaintiff had himself consented, there was no "willful" invasion of privacy, and therefore the claim failed. *See* Hollinsworth v. BCTV, [1998] BCJ No. 2451; 59 BCLR (3d) 121 at para. 29.

61 Chief Justice John Roberts of the US Supreme Court recently admitted that he "doesn't usually read the computer jargon that is a condition of accessing Web sites." *See* Debora Cassens Weiss, "Chief Justice Roberts Admits He Doesn't Read the Fine Print," *ABA Journal*, online: *http:// www.abajournal.com/news/article/chief_justice_roberts_admits_he_doesnt_read_the_computer_fine_print*.

62 For a discussion of these cases from a criminal law perspective, *see* Matthew Nied, "The Internet, Cloud Computing, and the Charter Right to Privacy: The Effect of Terms of Service Agreements on Reasonable Expectations of Privacy" (2011) 12:5 *Internet and E-Commerce Law in Canada* 40.

63 R. v. Ward, 2012 ONCA 660 [*Ward CA*].

64 *Id.* at para. 58.

65 R. v. Ward, 2008 ONCJ 355 at para. 46.

66 *Id.* at para. 68.

67 *Ward CA* at para. 52.

68 *Id.* at para. 108.

69 *Id.* at para. 78.

70 *Id.* at para. 109.

71 R. v. Cuttell, [2009] O.J. No. 4053 at paras. 30-33, 59, *aff'd* 2012 ONCA 661 at paras. 57-58, 126-128; R. v. Wilson, [2009] O.J. No. 1067 (S.C.J.) at paras. 35, 43; R. v. Vasic, [2009] O.J. No. 685; R. v. Trapp, [2009] S.J. No. 32 at para. 12 aff'd 2011 SKCA 143; 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]; R. v. Brousseau, [2010] O.J. No. 5793 at paras. 46, 50; R. v. McNeice, 2010 BCSC 1544 at para. 46; R. v. Spencer, [2009] S.J. No. 798, 2009 SKQB 341 at para. 19; R. v. James, [2013] O.J. No. 3591 at paras. 55-61 and 108-114; R. v. Thomas, [2013] A.J. No. 384 at paras. 26-29; R. v. Caza, [2012] B.C.J. No. 725 at para. 56. *See also Cuttell* 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* 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."

72 *See, e.g.*, *McNeice* at para. 46; *Friers* at para. 21; *see also Vasic* at paras. 55-56.

73 *See, e.g.,* McNeice.

74 *See, e.g., Vasic* at para. 46.

75 *Gomboc* at paras. 31 and 84.

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

77 *Id.* at para. 89.

78 *Id.* at para. 32.

79 *Id.* at para. 33.

80 *Id.* at paras. 58, 82, and 95.

81 *Id.* at para. 57.

82 *Id.* at para. 93.

83 *Id.* at para. 93.

84 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.).

85 Google's Privacy Policy of June 24, 2013, states that it "use[s] the information we collect from all of our services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and our users." *See* Google, *Privacy Policy*, online: *http:// www.google.com/intl/en/policies/privacy*. Google relies on language such as this as "consent." *See In re Google*, at 4.

17 No. 9 JINTLAW 3

End of Document