Privacy Class Actions: Before and After *Jones v. Tsige*

Nicole Henderson and Catherine Beagan Flood

In the seminal 2012 case *Jones v. Tsige*, the Ontario Court of Appeal for the first time confirmed the existence of “intrusion upon seclusion” as a valid cause of action in Ontario. The rationale for this incremental common law development was to fill a small, but important, gap in the law that would have left the plaintiff with no effective remedy for a deliberate and flagrant intrusion on her personal information by another individual. At the same time, in his reasons, Justice Sharpe cautioned against overreach and declined to recognize a cause of action wider than was needed to resolve the case before the Court of Appeal in *Jones*. He warned that a broader cause of action could “amount to an unmanageable legal proposition that would . . . breed confusion and uncertainty.”

In a paper written a year following the release of *Jones*, we noted that the new tort, as narrowly defined in *Jones*, did not lend itself to the certification of a class action in many circumstances, much less to success in a common issues trial. However, by 2014, it appeared that Justice Sharpe’s warning had largely fallen by the wayside as several privacy class actions were certified, relying on a very broad interpretation of *Jones* and the scope of the privacy tort it created.

In contrast to the intentional conduct sanctioned in *Jones*, privacy class actions are being certified in circumstances that undermine both the boundaries of the intrusion upon seclusion tort that were established in *Jones* and the carefully balanced statutory privacy regimes that pre-dated it. To date, appellate courts have done little to stem the proliferation of privacy class actions, including in cases where there is no “intrusion” to speak of and in which class members have not suffered losses that would ordinarily be compensable in tort.

---

2 See T.W. v. Seo, [2003] OJ No. 4277 (Sup Ct), varied on other issues, (2005) 256 DLR (4th) 1 (Ont CA) ("T.W. (CA)"); in which the defendant, an ultrasound technician, admitted videotaping the plaintiff in the change room of the defendant clinic at which he was employed, and conducting unauthorized examinations of her. While the individual defendant was found liable for battery, the Ontario Superior Court held: “After a review of the case law, I indicated that, in my opinion, insofar as a common law tort of invasion of privacy was recognized in Canada, it did not extend to these facts” (at para 22). It is difficult to imagine facts on which there would be a stronger argument that a tort of invasion of privacy should extend.
**Jones v. Tsige**

**Facts and judicial history**

Given the loose interpretation it has received in class action certification decisions since 2012, it is worth reviewing the facts and the legal reasoning of *Jones* in some detail. Both parties in this case were employees at the Bank of Montreal. Although they had never met, the defendant (Winnie Tsige) was involved in a relationship with the plaintiff’s (Sandra Jones’s) former spouse. It was not disputed that Tsige had improperly accessed the plaintiff’s personal banking records at least 174 times over a period of four years, contrary to bank policy. Tsige claimed that she was involved in a financial dispute with Jones’s former husband and accessed the accounts to confirm whether he was paying child support to Jones, but she did not publish, distribute or record Jones’s banking information.  

Jones commenced an action against Tsige, claiming damages for (among other things) invasion of privacy.

The parties each brought competing motions seeking summary judgment. The motions judge dismissed the plaintiff’s claim on the basis that Ontario law did not recognize a tort of breach of privacy. Jones appealed to the Court of Appeal.

**New tort**

Justice Sharpe, writing for a unanimous Court of Appeal, reviewed the case law in Ontario and noted that while a common law tort of invasion of privacy had never been recognized by a Canadian appellate court, courts had remained open to the possibility that one could exist. There were a number of prior Ontario cases in which the Court declined to strike pleadings alleging a tort of invasion of privacy, finding that it was not “plain and obvious” that such a claim could not succeed. The Court of Appeal also noted that causes of action relating to privacy have been recognized in other jurisdictions, including the United States, the United Kingdom, Australia and New Zealand. Four Canadian provinces — British Columbia, Manitoba, Saskatchewan and Newfoundland — had enacted legislation creating statutory causes of action for invasion of privacy.

Most American jurisdictions have recognized four categories of torts relating to invasion of privacy:

1) intrusion upon seclusion;

2) public disclosure of embarrassing private facts about the plaintiff;

3) publicity which places the plaintiff in a false light in the public eye; and

4) appropriation of the plaintiff’s name or likeness.

---

5  Ibid at paras 4-5.
6  2011 ONSC 1475, 333 DLR (4th) 566.
7  Jones, supra at para 25.
8  Ibid at paras 29-32.
9  Ibid at paras 52, 55, and 61-64.
10 See e.g. Shulman v. Group W Productions, Inc., 18 Cal 4th 200 at 231 (1998) (this tort “encompasses unconsented-to physical intrusion into the home, hospital room or other place the privacy of which is legally recognized, as well as unwarranted sensory intrusions such as eavesdropping, wiretapping, and visual or photographic spying”).
11 The Restatement (Second) of Torts provides (at § 652D), “One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.” Because American protection for the First Amendment (free speech) is so strong, this tort has been given relatively little scope. In the U.S., it is very difficult to hold a defendant liable for publishing something that is true, even if it is extremely private.
12 False light privacy is defined as follows: “One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if (a) the false light in which the other was placed would be highly offensive to a reasonable person, and (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed”. Restatement at § 652E. False light privacy overlaps to a large extent with other torts. False light claims could be treated as defamation where the plaintiff’s reputation is injured by a false statement, or as disclosure of private facts where the plaintiff argues that the statement, regardless of truth or falsity, has drawn unwanted public attention and therefore exposed his or her private life.
13 Ibid at paras 19-19.
As Justice Sharpe noted, the fourth, appropriation of personality, was already accepted as a cause of action in Ontario.  

In addition to these trends, the Court of Appeal cited three additional reasons to recognize a tort of intrusion upon seclusion. First, Justice Sharpe placed some emphasis on the fact that Canadian courts have long recognized that a right to privacy underlies certain rights under the Canadian Charter of Rights and Freedoms — including the right to be free from unreasonable searches — and further that the common law should develop in a manner consistent with the Charter. Secondly, technological advancements have led to the routine collection and electronic storage of vast amounts of highly personal information, posing a novel threat to the privacy of individuals.

Finally, a compelling consideration for the Court of Appeal was that absent recognition of a new cause of action, Jones would be left without an effective legal remedy against Tsige. The Personal Information Protection and Electronic Documents Act (PIPEDA) applies only to collection, use and disclosure of personal information for commercial purposes (or employment purposes in federally regulated industries). As a result, Jones’s recourse would have been limited to making a complaint to the Privacy Commissioner against the bank, which was holding her financial information for commercial purposes in addition to being her employer. She would have had no recourse directly against Tsige, who collected and used Jones’s personal information solely “for personal or domestic purposes” that are excluded from PIPEDA.

Against this background, the Court of Appeal confirmed the existence of a right of action for intrusion upon seclusion. This new tort has three elements, that:

1. the defendant’s conduct be intentional or reckless;
2. the defendant have invaded the plaintiff’s private affairs or concerns without lawful justification; and
3. a reasonable person would regard the invasion as highly offensive, causing distress, humiliation or anguish.

It is not necessary for the plaintiff to prove any harm to his or her economic interests. It is also not necessary that the plaintiff’s personal information have been published or disseminated by the defendant; the tort focuses on the act of intrusion upon the plaintiff’s private affairs, rather than subsequent use of the information.

The Court of Appeal was careful to emphasize that only “deliberate and significant invasions of personal privacy,” which would be viewed as offensive on an objective standard, will ground a cause of action. Accordingly, the Court suggested that only intrusion into highly personal matters, such as an individual’s financial or health records, sexual practices and orientation, employment, diary or private correspondence will meet the standard. The Court specifically excluded minor breaches, or claims by individuals who are overly sensitive about their privacy, from the ambit of the new tort.
Damages for intrusion upon seclusion

Since claims for invasion of privacy will usually involve intangible interests such as humiliation or emotional distress, as opposed to pecuniary losses, the Court of Appeal acknowledged that damages for intrusion upon seclusion will often be nominal. \(^{21}\) It imposed a cap of $20,000 where the plaintiff has suffered no pecuniary loss. \(^{22}\) While not precluding punitive or aggravated damages awards in “truly exceptional” cases, the Court was clear that it would not encourage them. \(^{23}\)

The factors identified for determining the quantum of damages were:

1. the nature, incidence and occasion of the defendant’s wrongful act;
2. the effect of the wrong on the plaintiff’s health, welfare, social, business or financial position;
3. any relationship, whether domestic or otherwise, between the parties;
4. any distress, annoyance or embarrassment suffered by the plaintiff arising from the wrong; and
5. the conduct of the parties, both before and after the wrong, including any apology or offer of amends made by the defendant. \(^{24}\)

Result

In the result, the Court of Appeal found that the defendant had committed the tort of intrusion upon seclusion and granted summary judgment in favour of the plaintiff. Damages were fixed at C$10,000, having regard to the factors set out above. The Court noted the deliberate and repeated nature of the defendant’s actions, the background of domestic relationships and the plaintiff’s distress at the invasion of her privacy. \(^{25}\) On the other hand, the plaintiff had not suffered any public embarrassment or harm to her health, welfare, social, business or financial position, and the defendant had apologized for her conduct and attempted to make amends. Despite the deliberate nature of the defendant’s conduct, the Court found that aggravated or punitive damages were not warranted. \(^{26}\)

Privacy Class Actions before Jones v. Tsige

Prior to Jones, privacy class actions were hampered by the fact that PIPEDA requires that: (i) a complaint to the Privacy Commissioner be made and disposed of before an application for damages can be brought; and (ii) such an application be commenced in Federal Court (which has no jurisdiction over tort claims against private-sector entities or individuals and thus is not a common venue for class actions). \(^{27}\)

The United States has a longer history of class actions being brought for invasion of privacy, both at common law and under a variety of statutes protecting the integrity of personal information. However, plaintiffs have generally not enjoyed success in these actions, which have proven quite vulnerable to defendants’ motions to dismiss. A common basis of the defendants’ attack is that the plaintiffs have not been able to establish any damages flowing from the alleged breach.

\(^{21}\) Ibid at para 71.
\(^{22}\) Ibid at para 87.
\(^{23}\) Ibid at para 88.
\(^{24}\) Ibid at para 88.
\(^{25}\) Ibid at para 87.
\(^{26}\) Ibid at para 90.
\(^{27}\) PIPEDA, supra at ss. 14 and 16.
A number of proposed class actions in the U.S. have been brought following data breaches, particularly by financial institutions. For example, in Pisciotta v. Old National Bancorp, the plaintiffs brought a proposed class action after a hacker obtained access to a database maintained by the defendant that contained confidential personal information, including names, addresses, social security numbers, credit card and other financial account numbers. While none of the class members claimed to have suffered any direct financial losses as a result of the breach, they claimed damages for ongoing credit monitoring. In upholding the lower court’s dismissal of the action, the U.S. Court of Appeals (Seventh Circuit) found that without more, an alleged increased risk of identity theft was not a legally compensable injury.

Similarly, in Giordano v. Wachovia Securities LLC, a putative class action was commenced after a report containing financial information about tens of thousands of the defendant’s customers was lost in transit. Among other causes of action, the plaintiff claimed invasion of privacy and breach of confidence, and sought damages for ongoing credit monitoring services to prevent identity theft. The New Jersey District Court allowed the defendant’s motion to dismiss for lack of standing, as the plaintiff’s claims were based on only a perceived risk of future harm that did not rise to the level of a “concrete and particularized injury.”

Though it did not discuss Jones v. Tsige, the Québec Superior Court applied similar reasoning in Mazzonna v. DaimlerChrysler Financial Services Canada Inc., denying authorization for a proposed class proceeding based on the loss of a data tape containing the personal information of approximately 240,000 individuals. The petitioner in that case did not allege that she had in fact been the victim of any fraud or identity theft arising from the data loss, but rather that she had experienced, as the Court summarized, “anxiety, inconvenience, pain, suffering and/or fear that she may be the target of fraud or identity theft,” as well as an increased risk of falling victim to fraud or identify theft.

Citing the Supreme Court of Canada’s decision in Mustapha v. Culligan of Canada Ltd., the Court found that these feelings did not rise to the level of a legally compensable injury, but rather constituted the type of “ordinary annoyances, anxieties, and fears that people living in society routinely . . . accept.” The Court distinguished an earlier case in which class action authorization had been granted in similar circumstances involving a data loss, noting that the petitioner in that case had in fact been the victim of identity theft. The Court in Mazzonna characterized other claims for “potential damages,” contingent on class members actually falling victim to fraud or choosing to pay for credit monitoring or similar services, as speculative, and declined to consider them in assessing the prima facie existence of damages.

In Ontario, class actions relating to data breaches prior to Jones were rare; however, publicly disclosed settlements seem to reflect similar principles of recovery. In Speevak v. Canadian Imperial Bank of Commerce, a class action was brought on behalf of bank customers whose banking information was inadvertently transmitted by facsimile to two third parties. As part of the settlement, the bank agreed to make a charitable donation. A claims process was also established for class members; however,
the Court noted, “It appears that in most, if not all, cases the release of personal information occurred without causing direct financial loss to members of the class. Nevertheless, to the extent that class members are able to prove damages, including general damages or damages attributable to identity theft, those damages will be recoverable in the arbitration process” (emphasis added). 36

Rowlands v. Durham Regional Health was a class action resulting from the loss of a USB key containing confidential health information for over 80,000 individuals. Despite the submissions of objectors who were of the view that every member of the class should be entitled to nominal compensation, the Court approved a settlement that would provide class members with compensation only for provable economic losses. 37 Notably, the settlement approval hearing took place nearly six months following the Court of Appeal’s judgment in Jones, although class certification had been granted in December 2011, prior to the Jones decision.

Privacy Class Actions after Jones v. Tsige

In Jones, the Court of Appeal expressly stated that harm to a recognized economic interest was not required to make out intrusion upon seclusion; indeed, the Court acknowledged that damages would usually be nominal. It is perhaps therefore not surprising that intrusion upon seclusion claims have been pleaded in a number of privacy class actions, in circumstances in which many if not all class members have apparently not suffered any tangible losses.

In one of our earlier papers, we identified two significant obstacles to establishing liability based on intrusion upon seclusion in typical data breach cases. First, the test set out in Jones requires the plaintiff to show that the defendant intruded upon her private concerns, which is simply not the case in many data breach situations — particularly those involving hacking or other deliberate cyber-attacks. 38 Second, there is a requirement that the invasion of the plaintiff’s privacy be “highly offensive” to persons of reasonable sensibility. While the unauthorized disclosure of any personal information may be distressing to some, many data breaches involve information with a significantly lower level of sensitivity (e.g., names, addresses, social insurance numbers), such that it would be difficult to characterize any intrusion as “humiliating” or an affront to one’s dignity.

Given the limitations of the intrusion on seclusion tort, security breaches are most amenable to redress under personal information protection legislation, such as PIPEDA, rather than through class actions. Nevertheless, as of the date of this publication, there have been several reported cases considering intrusion upon seclusion as a cause of action in the context of a class action. Unfortunately, each of these decisions represents something of a departure from the principles set out in Jones, raising the spectre of the very type of expanding and unmanageable cause of action that the Court of Appeal cautioned against when it recognized the new tort. Four of these cases — Hopkins v. Kay, Condon v. Canada, Evans v. Bank of Nova Scotia and Doe v. Canada — are discussed in turn below. 39

36 2010 ONSC 1128 at para. 43, 93 CPC (6th) 195.
37 2012 ONSC 3948 at paras. 11, 13, 30.
38 In Ludmer v. Ludmer, 2013 ONSC 794, [2013] ONCJ No 699, aff’d 2014 ONCA 827, [2014] OJ No 5565, the Court dismissed a claim for intrusion upon seclusion where there had been no such deliberate conduct on the part of the defendant. The plaintiff husband had brought a third party claim against a neighbour who had faxed emails the wife had intercepted from the husband’s account to the wife’s counsel, with the intention of assisting her in the litigation. The court held that the third party defendant’s conduct did not constitute a “deliberate and significant invasion of personal privacy,” having found as a fact that the neighbour had not hacked or improperly accessed the husband’s email account himself, nor had he read the emails. This finding was upheld by the Ontario Court of Appeal.
39 A fifth case, Murray v. Capital District Health Authority, 2015 NSC 61, [2015] NSJ No 77, certified a common issue for intrusion upon seclusion in the context of a mass strip search at a forensic psychiatry facility. While it is not clear that the new tort can or should be used to address issues relating to bodily integrity, the issues raised by Murray are outside of the scope of this paper.
Hopkins v. Kay

Hopkins v. Kay is a proposed class action involving unauthorized access and dissemination of certain health records by hospital employees. The plaintiffs allege that the medical records of approximately 280 hospital patients were wrongfully accessed by the defendants (the hospital and several of its employees, and a community college) and disseminated to unknown third parties. The plaintiffs commenced an action for intrusion upon seclusion, seeking damages for psychological harm and punitive damages. The hospital brought a preliminary motion to strike the plaintiffs’ claims on the basis that they disclosed no reasonable cause of action and that the courts have no jurisdiction over the claims.

The hospital had already acknowledged that the medical records were improperly accessed and had taken corrective action by apologizing to those affected and dismissing the employees involved. On the motion in Hopkins, however, the hospital’s position was that the subject matter of the plaintiffs’ claims fell squarely within the scope of the Personal Health Information Protection Act (PHIPA). It argued that PHIPA provides an exclusive, comprehensive code for privacy obligations and remedies for breach thereof in the health-care context, and that the Superior Court was therefore without jurisdiction to hear the plaintiff’s claims. Under PHIPA, an action for damages is only available once the Information and Privacy Commissioner of Ontario (Commissioner) has made an order that there has been a breach of the statute. Further, damages for mental anguish are capped at $10,000, half of the tentative threshold set by the Court of Appeal in Jones.

The motions judge rejected the hospital’s arguments and held that the class action could proceed, treating Jones as deciding broadly that a claim for intrusion upon seclusion should be permitted to proceed in Ontario. In doing so, the motions judge declined to follow a line of cases from British Columbia and Alberta finding that various provincial privacy statutes constitute a complete code that preclude common law claims for breach of privacy. He noted that in Jones, the Court of Appeal had considered the existence of other privacy statutes but nonetheless decided to recognize the new tort of intrusion upon seclusion; he characterized this discussion as relevant to the question of whether PHIPA had occupied the field with respect to claims based on unauthorized use of personal health information.

The hospital’s later appeal was dismissed; the Ontario Court of Appeal agreed with the plaintiffs that PHIPA did not displace the common law tort. While the motions judge had engaged in a relatively attenuated analysis of the effect of PHIPA on the applicability of the common law tort, this was the primary issue before the Court of Appeal and was addressed in great detail. As a matter of statutory interpretation, Justice Sharpe (writing for the Court) found that PHIPA did not create an exclusive procedure to address breaches of the Act, because in his view the statute specifically contemplates the existence of parallel court proceedings.

---

41 Hopkins SCJ, supra at para 7.
42 Establishing that the plaintiff’s claim discloses a reasonable cause of action is also the first criterion for certification of a class proceeding under s 5(1)(a) of the Class Proceedings Act, 1992, SO 1992, c 6.
43 Hopkins SCJ, supra at para 8.
44 Personal Health Information Protection Act, 2004, SO 2004, c 3 ["PHIPA"].
45 Hopkins SCJ, supra at para 10.
46 PHIPA, supra s. 65(1).
47 Ibid s. 65(3); Jones, supra at para 87.
48 Jones, supra at paras 28, 30.
50 Hopkins OCA, supra at paras 24-29.
51 Hopkins OCA, supra at paras 29-45.
Notably, the Commissioner intervened in the appeal in support of the plaintiffs’ position. Among other things, the Commissioner took the position that his focus was on “prevention, containment, investigation and the systemic remediation of contraventions of PHIPA” rather than the adjudication of individual complaints, although addressing both systemic and individual wrongs fall within his statutory powers.

While acknowledging that the Commissioner’s position could not bind the Court, the Court of Appeal appears to have given considerable weight to the Commissioner’s desire that he not be given exclusive jurisdiction over individual claims. Justice Sharpe also found that the Commissioner’s policy coincided with his reading of PHIPA, which he saw as focused on investigation into systemic issues.

The Court of Appeal is likely to have been influenced by the fact that the Commissioner had made no order under PHIPA, a precondition to a private action for damages under the statute. In Jones, the primary rationale for the recognition of a new tort was a lacuna in the law that would have left the plaintiff with no viable remedy. In Hopkins, the plaintiffs would have been able to seek recourse, including a potential claim for damages, under PHIPA, even if it was not their preferred procedure. Indeed, the plaintiffs had pleaded breach of PHIPA as one of several causes of action in their original statement of claim, but following amendments had chosen to rely only on intrusion upon seclusion.

The fact that the plaintiffs chose not to seek an adequate alternative remedy available to them through the PHIPA procedure (a complaint to the Commissioner followed by a private action under the statute) does not mean there is a gap in the law.

While it is perhaps not surprising that the plaintiffs would therefore prefer to pursue their claims under the common law tort given the availability of higher damages, the Court of Appeal’s decision gives rise to concerns that the tailored regime adopted by the Legislature to address privacy in the context of personal health information will be undermined if new privacy torts are gradually expanded as in Hopkins.

Perhaps more troublingly, the reasoning of Hopkins suggests some reshaping of the role of the Commissioner in investigating and addressing breaches of PHIPA. While the Commissioner has a clear statutory mandate to deal with individual complaints under PHIPA, the Court of Appeal in Hopkins appeared willing to allow the courts to assume this role, so the Commissioner could focus on other aspects of his duties.

Unfortunately, the Supreme Court of Canada has decided not to address these issues at this time. On October 29, 2015, the Supreme Court dismissed the defendants’ application for leave to appeal.

**Condon v. Canada**

In March 2014, the Federal Court certified a class proceeding in Condon v. Canada arising from the federal government’s loss of personal data of student loan recipients, including certifying a common issue on intrusion upon seclusion. The scope of this class action was expanded considerably by the Federal Court of Appeal in July 2015, to include claims based in negligence and breach of confidence.

In November 2012, Human Resources and Skills Development Canada (HRSDC) determined that it had lost an external hard drive containing the personal information of approximately 583,000 individuals who had participated in the Canada Student Loans program. The data on the hard drive included names, dates of birth, addresses, social insurance numbers and student loan balances. HRSDC had not been able to recover the hard drive or determine what had happened to it.
The plaintiffs commenced an action against the federal Crown relying on various causes of action including breach of contract (i.e., the class members’ student loan agreements), negligence, breach of confidence and intrusion upon seclusion. 59 The Crown’s position was that the plaintiffs’ claims did not disclose a reasonable cause of action because they had not suffered any compensable damages and that a class proceeding was not the preferable procedure to resolve class members’ claims. 60

HRSDC had acknowledged the data loss and offered affected individuals various fraud-prevention services. 61 However, no evidence was led on the certification motion to suggest that any class member had become the victim of identity theft or suffered any tangible loss. 62 The plaintiffs claimed that they had suffered inconvenience and expense in responding to the data loss and had been exposed to an increased risk of identity fraud. 63

With respect to intrusion upon seclusion, the Crown took the position that it had not “invaded” the plaintiffs’ private concerns, because HRSDC was lawfully in possession of the class members’ personal information, which they had voluntarily provided pursuant to their student loan agreements. 64 It also argued that the nature of the information contained on the hard drive was not sufficiently sensitive as to cause embarrassment or humiliation. 65

Dealing with the first argument, the Federal Court found that it was sufficient that the plaintiffs had alleged that the defendant had disclosed their personal information in an unlawful way and had not destroyed it in accordance with statutory requirements. 66 As to the nature of the information disclosed, the motions judge read Jones as requiring only that the disclosure of the information in issue cause distress, humiliation or anguish, not that the information itself be embarrassing or humiliating. 67 He also quoted the passage in Hopkins in which the Ontario Superior Court of Justice suggested that Jones should not be confined to its facts and that the Court of Appeal had acknowledged a broad right to proceed with a common law claim for breach of privacy. 68

The motions judge therefore found that the plaintiffs’ claim for intrusion upon seclusion disclosed a reasonable cause of action and was amenable to certification. In certifying such a claim in the absence of any “intrusion,” Condon represents an even bolder departure from Jones than Hopkins. On the facts pleaded in Condon, the motions judge accepted that HRSDC was lawfully in possession of the personal information in issue and had not taken any deliberate action to disclose or misuse it. 69 While there may have been a reasonable argument that HRSDC had not taken adequate care to safeguard the information, Condon seems to have equated negligence (absent the requirement of compensable damages) with intrusion upon seclusion, which is incompatible with the intentional nature of the tort as enunciated by the Court of Appeal in Jones.

Condon also appears to have distorted the requirement from Jones that the Court have regard to the nature of the information intruded upon to assess whether the invasion of the plaintiff’s private affairs be of a nature that would cause a reasonable person “distress, humiliation or anguish.” While not purporting to be exhaustive, Jones set out a list of subject matters of personal information upon which an intrusion

---

59 Ibid at para 30.
60 Ibid at para 4.
61 Ibid at paras 17-20.
62 Ibid at paras 68-69.
63 Ibid at para 66.
64 Ibid at para 55. See also Connolly v. Telus Communications Co, [2012] OJ No 464 (Small Claims Ct) (QL), in which the plaintiff alleged that Telus had mishandled his Social Insurance Number (SIN) during its account registration process. In obiter, the trial judge concluded that the plaintiff would not be able to recover damages for intrusion upon seclusion, in particular since there had been no “intrusion,” given that the plaintiff had voluntarily provided his SIN to Telus.
65 Condon FC, supra at para 56.
66 Ibid at para 58.
67 Ibid at para 60.
68 Ibid at para 63.
69 Condon FC, supra at para 58.
would be considered “highly offensive” — including medical records and private correspondence — all of which are more personally sensitive than core biographical information such as a person’s name and address. Although Justice Sharpe referred generally to such categories as “financial records” in his reasons in *Jones*, in our view the totality of the reasons make clear that intrusion of seclusion will only be made out when the information intruded upon reaches an objective threshold of sensitivity. In contrast, in *Condon*, the Federal Court gave a very cursory consideration to the nature of the information disclosed, and instead focused on whether HRSDC’s failure to protect the plaintiffs’ personal information would cause distress, humiliation or anguish, an analysis that again focuses on alleged negligence as opposed to deliberate action in respect of embarrassing information.

With respect to negligence and breach of confidence, the motions judge followed *Mazzonna* and held that the absence of compensable damages was fatal to the plaintiff’s claims in negligence and breach of confidence, and that these did not disclose a reasonable cause of action.

Despite their overall success in having the action certified, the plaintiffs appealed the motions judge’s refusal to certify these claims (the government abandoned its cross appeal). The Court of Appeal held that the motions judge should have analyzed the issue based only on the allegations made in the statement of claim, which alleged that class members had sustained damages in the form of “costs incurred in preventing identify theft” and unspecified “out-of-pocket expenses.”

The appellate court considered these pleadings of damages to be sufficient for the purposes of the certification criteria and that there was therefore no basis not to include the claims in negligence and breach of confidence in the class proceeding. It did not consider any of the other certification criteria, particularly whether there was some basis in fact that the claims in negligence and breach of confidence presented common issues of fact or law. While the pleadings are to be taken as true for the purposes of evaluating whether they disclose a reasonable cause of action and a certification judge is not permitted to scrutinize the merits of the case, a complete absence of evidence that class members suffered damages would usually be relevant to the common issues criterion. In this regard, the Court’s omission was surprising.

Notably, in its brief reasons, the Court of Appeal did not address the application of *Mazzonna* or any of the other Canadian and U.S. cases that have held that mere exposure to a risk of identity theft or fraud is not a compensable injury in the absence of some provable loss. The court also did not query whether the plaintiffs’ alleged damages were a recoverable form of pure economic loss.

To date, *Condon* has not received any detailed judicial consideration. If it is followed, its reasoning risks shifting intrusion upon seclusion from a dignity-based tort to a risk-based one focused on preventing inadequate protection of personal data by organizations. There is nothing in *Jones* to suggest that this is what the Ontario Court of Appeal contemplated. Moreover, the Federal Court of Appeal’s expansion of the claims certified reflects a troubling departure from prior case law with respect to torts that require proof of damages for recovery. Although nominal damages may be available in respect of intrusion on seclusion (where it is properly made out), tort law has traditionally been focused much more squarely on redressing tangible losses. The approach in *Condon* risks turning this role on its head.

---

70 *Jones*, supra at para 72.
71 *Condon*, supra at para 60.
72 See also *Sofio c. Organisme canadien de réglementation du commerce des valeurs mobilières (OCRCVM)*, 2014 QCCS 4061, which also applied *Mazzonna* to deny authorization (certification) to a proposed class proceeding arising out of the loss of a laptop computer containing the personal information of approximately 50,000 customers of a number of brokerage firms. The petitioner did not claim that he had suffered any pecuniary loss but claimed damages for stress and inconvenience. Relying on *Mazzonna* and Mustapha, supra, the Court found that he had not suffered any compensable injury, which was fatal to his claim.
73 *Condon FCA*, supra paras 17-18.
74 Ibid at para 22.
Evans v. The Bank of Nova Scotia

Evans v. The Bank of Nova Scotia\(^{75}\) involved allegations that a rogue bank employee (Richard Wilson) had improperly accessed the banking records of at least 643 customers of Scotiabank.\(^{76}\) The employee provided some of this personal information to his girlfriend, who in turn disclosed it to third parties for fraudulent purposes; there was evidence that at least 138 of the bank’s customers had fallen victim to some form of identity theft or fraud as a result. Although the bank had compensated all victims who suffered pecuniary losses as a result of this fraud, the plaintiffs sought certification of a class proceeding on behalf of all customers whose information had been improperly accessed.\(^{77}\)

Unlike Jones, the plaintiffs named both the employee and the bank as defendants in their action, relying on various causes of action including negligence and intrusion upon seclusion.\(^{78}\) The employee did not defend the action and was noted in default.\(^{79}\) The plaintiffs claimed that the bank was vicariously liable for the employee’s intrusion upon seclusion, as well as directly liable for negligently failing to supervise his access to and use of customer information.\(^{80}\) They acknowledged that the bank was not directly liable for intrusion upon seclusion, because there was no intentional action on its part with respect to Wilson’s disclosure of their personal information.\(^{81}\)

As there did not appear to be any dispute that the employee had committed an intrusion on seclusion, the Court’s analysis focused on whether the claim that the bank was vicariously liable for his tort disclosed a reasonable cause of action. Vicarious liability is a form of strict liability whereby an employer may be held jointly and severally liable for the tortious act of an employee, notwithstanding that the conduct was not authorized and that the employer was not otherwise at fault.\(^{82}\) As set out in Bazley v. Curry, the fundamental question is whether the employee’s wrongful act is sufficiently related to conduct authorized by the employer to justify imposition of this type of liability.\(^{83}\)

On the facts of Evans, the motions judge held that the claim against the bank based in vicarious liability disclosed a reasonable cause of action.\(^{84}\) Bazley set out five factors to assess whether vicarious liability should be imposed for an intentional tort:

1) the opportunity that the enterprise afforded the employee to abuse his or her power;  
2) the extent to which the wrongful act may have furthered the employer’s aims (and hence be more likely to have been committed by the employee);  
3) the extent to which the wrongful act was related to friction, confrontation or intimacy inherent in the employer’s enterprise;  
4) the extent of power conferred on the employee in relation to the victim; and  
5) the vulnerability of potential victims to wrongful exercise of the employee’s power.\(^{85}\)

The motions judge found that the bank had created the opportunity for the employee’s abuse by allowing unsupervised access to customers’ personal information.\(^{86}\)

---

\(^{76}\) Ibid at para 4.  
\(^{77}\) Ibid at paras 65-67.  
\(^{78}\) Ibid at para 12.  
\(^{79}\) Ibid at para 17.  
\(^{80}\) Ibid at para 12.  
\(^{81}\) Ibid at para 19.  
\(^{82}\) T.W. (CA), supra at para 39 (Ont CA).  
\(^{83}\) [1999] 2 SCR 534 at para 41.  
\(^{84}\) Evans, supra at para 30.  
\(^{85}\) Ibid at para 21, citing Bazley v. Curry, supra at para 41.  
\(^{86}\) Evans, supra at paras 22-23.
Unfortunately, the Court’s analysis of the vicarious liability issue was fairly cursory, despite being the first case to deal with this question in the context of the tort of intrusion upon seclusion. The motions judge did not discuss in any detail the nature of the employee’s duties and his relationship (if any) with class members, rather, his reasons focused on the opportunity created by the bank’s lack of monitoring, which is more appropriate in the context of the analysis of the bank’s direct liability as opposed to vicarious liability. Even if the alleged enterprise-wide lack of supervision enabled the employee to improperly access and disclose class members’ personal information, that does not necessarily translate into the “strong connection” required between the wrong done to a particular plaintiff and the duties of the particular employee.

The motions judge in Evans also did not engage in the policy analysis prescribed in Bazley where the imposition of vicarious liability is sought in circumstances not falling within established precedents. In particular, with respect to the deterring effect of vicarious liability, the Supreme Court of Canada has emphasized that deterrence should be limited to situations where it can be effective and that courts should be cautious about over-deterrence of “activities which are socially useful and ought to be promoted rather than penalized.” As the Ontario Court of Appeal recognized in Jones, the collection and electronic storage of personal information has become increasingly routine. While this may raise new privacy concerns, it is also in most cases economically useful and efficient activity that, in our view, courts should be reluctant to deter more broadly than necessary to protect the values underlying the new privacy tort. Indeed, the alternative is increased monitoring and thus less privacy for employees.

**Doe v. Canada**

*Doe v. Canada*, released July 27, 2015, is the second privacy class action certified by the Federal Court — a court that, as we note above, has traditionally not been a common venue for class actions. This case involved an alleged privacy breach affecting participants in the federal government’s Marihuana Medical Access Program (MMAP). Health Canada acknowledged that in November 2013, contrary to its usual practices, it sent participants in the MMAP correspondence in oversize envelopes bearing the name of the program as part of the return address. The plaintiffs alleged that seeing the envelopes would cause a reasonable person to conclude that the addressee suffers from a grave or debilitating medical condition (which would make him or her eligible to participate in the MMAP) and possesses and consumes marihuana.

The federal Privacy Commissioner had already issued a report in March 2015 finding that the complaints of a number of MMAP participants in respect of this action were well-founded and that Health Canada’s conduct violated the *Privacy Act*. Although the plaintiffs relied on that report at the certification hearing, they did not seek certification of any common issues for breach of the *Privacy Act* — they pleaded breach of contract, negligence, breach of confidence, intrusion on seclusion, “publicity given to private life” and breaches of sections 7 and 8 of the *Canadian Charter of Rights and Freedoms*.

87 See also Leung v. Shanks, 2013 ONSC 4943 at para 41; and Ari, supra at paras 66-79, where the Court declined to strike a claim for vicarious liability in a privacy breach case, applying similar reasoning regarding the opportunity afforded to an employee to abuse her power to access personal information of her employer’s customers. The Court noted that the “opportunity” was the only factor pleaded by the plaintiff to establish vicarious liability, but held that while this might weaken the vicarious liability claim, it was not plain and obvious that it could not succeed.
89 See *ibid* at paras 4, 21-22.
90 *ibid* at para 55.
91 Jones, supra at paras 67-68.
93 *ibid* at para 20.
94 *ibid* at para 15.
95 *ibid* at paras 28, 50.
The motions judge concluded fairly swiftly that all of the claims pleaded, with the exception of the Charter claims, disclosed a reasonable cause of action. The Court followed the Federal Court of Appeal’s decision Condon for the proposition that in respect of the claims in negligence and breach of confidence, it was sufficient for the plaintiffs to plead the general type of damage alleged and that they did not need to establish that every class member had suffered damages. It held that the claim for intrusion upon seclusion was adequately pleaded. Most notably, the Court permitted the claim for “publicity given to private life” — the second category of privacy tort recognized in the U.S. — to proceed on the basis that it was novel and should not be struck at an early stage of the litigation. Despite the cautious and incremental approach to the recognition of new privacy torts evinced in Jones, the Court did not engage in any substantive analysis of whether this claim had a chance of success on the facts pleaded.

The motions judge also found broadly that the Privacy Commissioner’s report on this incident provided some basis in fact for the action, treating the “some basis in fact” as a threshold issue that permitted the court to go on to consider the other certification criteria. In its analysis of the common issues criterion, the Court did not consider whether there was some basis in fact for each of the common issues alleged, an approach that resembled the Federal Court of Appeal’s reasoning in Condon, but rather focused on whether resolution of the common issues would advance the litigation.

Doe is another case, like Condon, where there is no evidence that class members had suffered any damages and not even evidence of any “intrusion.” While Health Canada’s conduct allegedly did not comply with the Privacy Act, the government did not improperly obtain access to class members’ private information or affairs. The information in issue was provided to Health Canada and was not alleged to have been used for any purpose other than administering the MMAP. Moreover, the Court did not refer to any evidence that the envelopes had been seen by anyone other than Canada Post employees. It is surprising that the plaintiff was found to have met the burden of showing some basis in fact for each of the common issues alleged.

A unique feature of Doe was that the proposed representative plaintiffs both wished to remain anonymous in order to avoid further disclosure of their participation in the MMAP. The government argued that individuals who were not prepared to be publicly identified as associated with the action could not be appropriate representative plaintiffs. Although he did not deny certification for this reason, the motions judge indicated that it was his intention that “if feasible,” at least one public representative plaintiff should be identified. Class counsel had apparently indicated to the Court that this likely would be feasible. However, given the nature of the interests at stake in privacy class actions, courts may need to grapple more fully with such requests for anonymity in future cases.

---

96 Ibid at paras 31-46.
97 Ibid at paras 34-36.
98 Ibid at paras 39-40.
99 Ibid at para 42. The motions judge relied on the Manitoba Court of Appeal’s decision in Grant v. Winnipeg Regional Health Authority, 2015 MBCA 44, as “recognizing” the tort of publicity given to private life. However, that case only acknowledged that the plaintiffs might have a claim for “publicity which places the individual in a false light in the public eye”—a different category of privacy tort recognized in the U.S.—if the facts alleged were proven (para 126). It did not purport to recognize any new tort.
100 Doe, supra at para 27.
101 Ibid at paras 51-52.
102 See ibid at para 22.
103 Ibid at para 5.
104 Ibid at para 60.
105 Ibid at para 63.
106 Ibid at para 62.
Conclusion

After almost four years, meaningful judicial consideration of Jones remains surprisingly sparse, despite the certification of several class actions that include intrusion upon seclusion as a common issue. In the field of class actions, two concerning trends appear to be emerging: first, the fairly casual extension of intrusion upon seclusion despite the Court of Appeal’s warning against such expansion in Jones; and second, the expansion of the common law breach of privacy tort in a manner that trenches upon long-established and carefully tailored statutory regimes aimed at protecting personal information. It is undeniable — as Jones recognized — that the widespread electronic collection and storage of information have made privacy an increasingly pressing concern for many. However, in our view, courts should be cautious about transforming a relatively constrained cause of action recognized in order to meet a narrow lacuna in the law of privacy into a salve for any and all alleged privacy breaches, particularly where there are other more appropriate tools available.

We note that the courts are not permitted to engage in meaningful consideration of the merits of an action at the certification stage. It remains to be seen whether plaintiffs will ultimately recover damages for intrusion upon seclusion once trial judges begin examining some of these issues with the benefit of a full record. However, given the significance of certification of a class proceeding against an organization, potential defendants would be wise to heed the old adage that an ounce of prevention is worth a pound of cure. The common thread running through all of the privacy class actions certified to date is the need for effective controls on how personal information may be accessed and used within organizations. The failure to impose adequate safeguards in this regard may leave employers vulnerable to what appears to be an expanding risk of class action litigation.

CONTACTS

Catherine Beagan Flood
Partner | Toronto
cbe@blakes.com
416-863-2269

Nicole Henderson
Associate | Toronto
nicole.henderson@blakes.com
416-863-2399