Privacy Class Actions Five Years after *Jones v. Tsige* – Key Ontario and Federal Court Decisions

The Advocates' Society Cybersecurity and Privacy Law for Litigators Program (Oct. 23, 2017)
Catherine Beagan Flood and Nicole Henderson[1]
Blake, Cassels & Graydon LLP

It has been five years since the seminal 2012 case *Jones v Tsige*, in which the Ontario Court of Appeal for the first time confirmed the existence of "intrusion upon seclusion" as a valid cause of action in Ontario.[2] Since 2012, there has been a proliferation of privacy class actions, including in cases in which there was no "intrusion" to speak of, and class members have not suffered losses that would ordinarily be compensable in tort. Recently, however, there have been some nascent signals that courts will be prepared to take a closer look at privacy class actions and assess whether the plaintiffs can establish all of the elements of the causes of action being relied on in these cases. Although it is unlikely that the tide of privacy class actions will be stemmed anytime soon, there is cause for some cautious optimism for defendants on the merits front.

Below, we discuss *Jones v Tsige* and six of the most significant subsequent Ontario and Federal Court privacy class action decisions.

1) 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.[3] Jones commenced an individual action (not a class proceeding) 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.[4] 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.[5]

---

[1] The authors would like to thank Jessica Lam, Associate, Blake, Cassels & Graydon LLP for her assistance in updating this paper.
[2] 2012 ONCA 32 108 OR (3d) 241, [2014] OJ No 148 ["*Jones*"].
[3] *Ibid* at paras 4-5.
[4] 2011 ONSC 1475, 333 DLR (4th) 566.
[5] *Jones, supra* at para 25.

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

1) intrusion upon seclusion;[6]
2) public disclosure of embarrassing private facts about the plaintiff;[7]
3) publicity which places the plaintiff in a false light in the public eye;[8] and
4) appropriation of the plaintiff's name or likeness.[9]

As Justice Sharpe noted, the fourth, appropriation of personality, was already accepted as a cause of action in Ontario.[10]

A compelling consideration for the Court of Appeal in recognizing a new privacy tort 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.[11]

---

[6] 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").

[7] 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.

[8] 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.

[9] *Ibid* at paras 18-19.

[10] *Ibid* at paras 24-28. See e.g. *Krouse v Chrysler Canada Ltd* (1974), 1 OR (2d) 225 (CA); *Athans v Canadian Adventure Camps Ltd* (1977), 17 OR (2d) 425 at p 434 (HCJ). See also *Aubry v Vice Versa*, [1998] 1 SCR 591 (damages awarded under *Quebec Charter of Human Rights and Freedoms* where photographs taken (in a public place) and published without consent.

[11] *Personal Information Protection and Electronic Documents Act*, SC 2005, c 5, s 4(2)(b) [*PIPEDA*]. Interestingly, Justice Sharpe also suggested that damages are not available as a remedy under *PIPEDA*. *PIPEDA* does in fact allow for an application to the Federal Court for damages, including damages for an individual's humiliation resulting from an organization's failure to comply with certain obligations under the Act (after the Privacy Commissioner has investigated the complaint and delivered a report, or has discontinued her investigation, per sections 14 and 16 of *PIPEDA*). Justice Sharpe may have been

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

1) the defendant's conduct be intentional or reckless;
2) the defendant must 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.[12]

It is not necessary for the plaintiff to prove any harm to his or her economic interests.[13] 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.[14]

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.[15] It imposed a cap of $20,000 where the plaintiff has suffered no pecuniary loss.[16] While not precluding punitive or aggravated damages awards in "truly exceptional" cases, the Court was clear that it would not encourage them.[17]

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.[18]

---

referring to the fact that, in this case, no damages would be available against the defendant (an individual who was not acting for a commercial purpose) under *PIPEDA*.

[12] *Jones, supra* at para 71.
[13] *Ibid*.
[14] *Ibid* at para 72.
[15] *Ibid* at para 71.
[16] *Ibid* at para 87.
[17] *Ibid* at para 88.
[18] *Ibid* at para 87.

Application to the facts

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 $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.[19] 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.[20]

2) Hopkins v Kay

Hopkins v Kay[21] 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.[22] 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.[23]

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.[24] 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*

---

[19] Compare *Peters-Brown v Regina District Health Board*, (1995), [1996] 1 WWR 337 (Sask QB), aff'd (1996), [1997] 1 WWR 638 (Sask CA), in which damages of C$5000 were awarded to the plaintiff prison guard, after she discovered that co-workers had a typewritten list prepared by Regina General Hospital of "previously identified cases" with whom body fluid precautions should be taken, which included her name. The plaintiff claimed that she suffered mental anguish as a result of disclosure to her fellow workers of the fact that she had been treated for a communicable disease (hepatitis B), and because her co-workers assumed that she posed a health risk to them (potentially AIDS). An award of C$5000 for breach of contract for failure to maintain the confidentiality of medical records and negligence was upheld by the Saskatchewan Court of Appeal, which concluded that medical evidence of nervous shock was not necessary. See also *McIntosh v Legal Aid Ontario*, 2014 ONSC 6136, [2014] OJ No 5216, in which the Court assessed damages of C$7500 against an individual defendant for intrusion upon seclusion. The defendant (who had been noted in default) was an employee of Legal Aid Ontario who allegedly improperly accessed the plaintiff's legal aid file. The court was not satisfied that the defendant had disclosed the plaintiff's personal information to the Children's Aid Society (in addition to accessing it) as pleaded in the statement of claim. The court found that the plaintiff had not suffered any economic losses but awarded general damages to reflect the "annoyance, anxiety, and distress" caused by the defendant's actions.

[20] *Ibid* at para 90.

[21] 2014 ONSC 321, [2014] OJ No 485 ["*Hopkins SCJ*"], aff'd 2015 ONCA 112 ["*Hopkins OCA*"], leave to appeal to SCC refused, [2015] SCCA No 157.

[22] *Hopkins SCJ, supra* at para 7.

[23] 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.

[24] *Hopkins SCJ, supra* at para 8.

Protection Act (PHIPA).[25] 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.[26] 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.[27] Further, damages for mental anguish are capped at $10,000, half of the threshold set by the Court of Appeal in *Jones*.[28]

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.[29] 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. 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.[30]

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,[31] even though addressing both systemic and individual wrongs fall within his statutory powers.[32] While acknowledging that the Commissioner's position could not bind the Court,[33] 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 own reading of PHIPA, which he saw as focused on investigation of systemic issues.[34]

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 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 later amended to rely only on intrusion upon seclusion.[35] 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) is not equivalent to the gap in the law that motivated *Jones v Tsige*.

While it is not surprising that the plaintiffs would prefer to pursue their claims under a common law tort that makes larger damages awards available, the Court of Appeal's decision gives rise

---

[25] *Personal Health Information Protection Act, 2004*, SO 2004, c 3 ["*PHIPA*"].
[26] *Hopkins SCJ, supra* at para 10.
[27] *PHIPA, supra* s 65(1).
[28] *Ibid* s 65(3); *Jones, supra* at para 87.
[29] *Jones, supra* at paras 28, 30.
[30] *Hopkins OCA, supra* at paras 39-45.
[31] *Ibid* at para 56.
[32] *Ibid* at paras 55, 57; *PHIPA, supra* ss 56-57.
[33] *Hopkins OCA, supra* at para 58.
[34] *Ibid* at para 38.
[35] *Hopkins SCJ, supra* at paras 2-3.

to concerns that the tailored regime adopted by the Legislature to address privacy in the context of personal health information will be undermined.

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 appeared willing to allow the courts to assume this role, so the Commissioner could focus on other aspects of his statutory duties.

3) 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 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.[36] The data on the hard drive included names, dates of birth, addresses, social insurance numbers and student loan balances.[37] 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.[38] 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.[39]

HRSDC had acknowledged the data loss and offered affected individuals various fraud-prevention services.[40] 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.[41] 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.[42]

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

---

[36] *Condon v Canada*, 2014 FC 250, [2014] FCJ No 297 at para 2 ["*Condon FC*"], varied 2015 FCA 159 ["*Condon FCA"*].
[37] *Ibid.*
[38] *Ibid* at para 30.
[39] *Ibid* at para 4.
[40] *Ibid* at paras 17-20.
[41] *Ibid* at paras 68-69.
[42] *Ibid* at para 66.

loan agreements.[43] It also argued that the nature of the information contained on the hard drive was not sufficiently sensitive as to cause embarrassment or humiliation.[44]

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.[45] 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.[46] 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.[47]

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.[48] 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 plaintiffs' 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 categories of personal information (e.g. medical records) considered "highly offensive" to intrude upon. All of these categories are much more personally sensitive than basic biographical information such as a person's name and address.[49] Although Justice Sharpe referred to general categories such 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 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.[50]

---

[43] *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.
[44] *Condon FC, supra* at para 56.
[45] *Ibid* at para 58.
[46] *Ibid* at para 60.
[47] *Ibid* at para 63.
[48] *Condon FC, supra* at para 58.
[49] *Jones, supra* at para 72.
[50] *Condon, supra* at para 60.

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 plaintiffs' claims in negligence and breach of confidence, and that these did not disclose a reasonable cause of action.[51]

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."[52]

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.[53] 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. The Court of Appeal'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 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.[54] 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.

---

[51] See also *Sofio c Organisme canadien de réglementation du commerce des valeurs mobilières (OCRCVM)*, 2014 QCCS 4061, aff'd 2015 QCCA 1820, 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.

[52] *Condon FCA, supra* paras 17-18.

[53] *Ibid* at para 22.

[54] In *Tucci v Peoples Trust Company*, 2017 BCSC 1525, the plaintiff relied on *Condon* in asserting that damages "including time-consuming, inconvenient, frustrating measures required to determine whether their Personal Information was involved in the Breach, and further steps to protect themselves from identify theft" were properly pleaded. The British Columbia Supreme Court accepted the plaintiff's position and held that it was not plain and obvious that costs incurred in preventing identify theft and damage to credit reputation could not constitute a compensable harm.

4) Evans v The Bank of Nova Scotia

Evans v The Bank of Nova Scotia[55] involved allegations that a rogue bank employee (Richard Wilson) had improperly accessed the banking records of at least 643 customers of Scotiabank.[56] Mr. Wilson 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.[57]

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.[58] The employee did not defend the action and was noted in default.[59] 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.[60] 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.[61]

As there did not appear to be any dispute that Wilson 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.[62] 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.[63]

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.[64] *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.[65]

---

[55] 2014 ONSC 2135, [2014] OJ No 2708, leave to appeal ref'd 2014 ONSC 7249, [2014] OJ No 6014 (Div Ct) ["*Evans*"].
[56] *Ibid* at para 4.
[57] *Ibid* at paras 65-67.
[58] *Ibid* at para 12.
[59] *Ibid* at para 17.
[60] *Ibid* at para 12.
[61] *Ibid* at para 19.
[62] T.W. v Seo, (2005) 256 DLR (4th) 1 (Ont CA) at para 39.
[63] [1999] 2 SCR 534 at para 41.
[64] *Evans, supra* at para 30.

The motions judge found that the bank had created the opportunity for the employee's abuse by allowing unsupervised access to customers' personal information.[66]

Unfortunately, the Court's analysis of the vicarious liability issue was fairly cursory,[67] 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.[68] 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.[69]

The motions judge in *Evans* also did not engage in the policy analysis prescribed in *Bazley* for cases in which vicarious liability is sought to be imposed in circumstances not falling within established precedents. In particular, 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."[70] As the Ontario Court of Appeal recognized in *Jones*, the collection and electronic storage of personal information has become increasingly routine.[71] 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.

5) Doe v Canada

Doe v Canada is the second privacy class action certified by the Federal Court. 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 envelopes bearing the name of the program as part of the return address.[72] The plaintiffs alleged that seeing the envelopes would cause a reasonable person to conclude that the addressee suffers

---

[65] *Ibid* at para 21, citing *Bazley v Curry, supra* at para 41.
[66] *Evans, supra* at paras. 22-23.
[67] 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. This aspect of the Court's decision was affirmed on appeal.
[68] *EB v Order of the Oblates of Mary Immaculate in the Province of British Columbia*, 2005 SCC 60, [2005] 3 SCR 45 at paras 4, 51-52 ["*EB*"].
[69] See *ibid* at paras 4, 21-22.
[70] *Ibid* at para 55.
[71] *Jones, supra* at paras 67-68.
[72] *Doe v Canada*, 2015 FC 916 at para 11 ["*Doe FC*"], reversed in part 2016 FCA 191 ["*Doe FCA*"].

from a grave or debilitating medical condition that would make him or her eligible to participate in the MMAP, and possesses and consumes marihuana.[73]

The federal Privacy Commissioner had already issued a report in March 2015 finding that the complaints of a number of MMAP participants were well-founded and that Health Canada's conduct violated the *Privacy Act*.[74] 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*.[75]

Following the Federal Court of Appeal's decision in *Condon*, 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.[76] 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.[77] 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. It also chose to recognize the new tort notwithstanding that it had already found that the plaintiffs had other viable claims against the defendant for the alleged privacy breach. This aspect of the Court's reasoning also separates it from *Jones*, in which the Ontario Court of Appeal felt compelled to recognize a new cause of action to prevent leaving a wronged plaintiff without a remedy.

The Crown appealed the Federal Court's decision, and the Federal Court of Appeal's judgment was released in June 2016. As in *Condon*, the Court of Appeal narrowed the scope of the action on appeal, finding that only the claims in negligence and breach of confidence should proceed. The Court of Appeal was critical of the motions judge for relying on the Privacy Commissioner's report as providing some basis in fact for the action, treating "some basis in fact" as merely a threshold issue that permitted the court to go on to consider the other certification criteria.[78] As the Court of Appeal pointed out, the motions judge should have considered whether there was some basis in fact for each of the common issues put forward for certification.[79]

Puzzlingly, then, the Court of Appeal affirmed that for purposes of the negligence and breach of confidence claims, it was sufficient for the plaintiffs to have pleaded the "nature of any damages claimed".[80] *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 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 lawfully provided to

---

[73] *Ibid* at para 20.
[74] *Ibid* at para 15.
[75] *Ibid* at paras 28, 50.
[76] *Ibid* at paras 31-46.
[77] *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.
[78] *Doe FC, supra* at para 27; *Doe FCA, supra* at para 36.
[79] *Doe FCA, supra* at para 37.
[80] *Doe FCA, supra* at paras 50-51

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.[81] It is surprising that the plaintiffs were found to have met the burden of showing some basis in fact for those claims that require proof of damages for recovery.

However, the Court of Appeal did conclude that the plaintiffs' claims for intrusion upon seclusion did not disclose a reasonable cause of action because they had not alleged that the defendant's conduct was intentional, reckless, or done in bad faith. Rather, it observed that "at best, the material facts pleaded support the notion that an isolated administrative error was made. This is a far cry from the situation in *Tsige*, where a bank employee accessed private financial information…in order to maintain surveillance over her former spouse and his new partner; moreover, Ms. Tsige was aware that her actions were wrong."[82]

With respect to the motions judge's recognition of the tort of publicity given to private life, the Court of Appeal briefly reasoned that the cause of action should not be dismissed simply because it is novel. It found that the plaintiff's claim could not proceed because it was not pleaded that the information in issue was "communicated to the public at large," which the Court of Appeal construed as an essential element of the tort as framed in the US jurisprudence.[83]

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.[84] 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.[85] The Court of Appeal was stronger in its reasons, holding that "the anonymity of class representatives is at odds" with the responsibilities of a representative plaintiff.[86] It nonetheless seemed to leave open the possibility that the class could return to the court for directions in the event that no one came forward who was prepared to be publicly named as a representative plaintiff.[87] In *Doe,* it does not appear that this will be an issue.[88] 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.

6) Lozanski v Home Depot Inc.

Lozanski is the first class action involving allegations of intrusion upon seclusion to be settled on a class-wide basis. This case arose out of a data breach involving Home Depot, in which the email addresses of up to half a million Canadian customers may have been obtained by criminal

---

[81] See *Doe FC, supra* at para 22.
[82] *Doe FCA, supra* at para 58.
[83] *Doe FCA, supra* at paras 53-56. This interpretation is at odds with the decision of the Ontario Small Claims Court in *Halley v McCann*, [2016] OJ No 4672, where the court found that communication of private information to only three people was sufficient to found liability for publication of embarrassing private facts (at para 25). In *Halley*, the Court relied on an earlier decision of the Ontario Superior Court, *Jane Doe 464533 v ND*, 2016 ONSC 541 as recognizing this tort—that case involved a defendant who had unquestionably "published" intimate images of the plaintiff on the internet. The defendant in *Halley* did not deny that her disclosures were acts of publication.
[84] *Doe FC, supra* at para 5.
[85] *Ibid* at para 63.
[86] *Doe FCA, supra* at para 75.
[87] *Ibid* at para 77.
[88] *Ibid.*

intruders who compromised the company's computer system.[89] Home Depot had immediately responded to the breach by notifying customers and a number of Privacy Commissioners, issuing an apology, and offering credit monitoring to affected customers.[90]

The *Lozanski* action was commenced in September 2014, although by the time of the settlement approval motion in August 2016, there was no evidence that any class member had fallen victim to fraud or identity theft as a result of the breach.[91]

The settlement agreement provided for further funding for credit monitoring (up to a cap of $250,000) and compensation of up to $5000 for any class members with documented losses (including time spent remedying issues relating to the breach).[92] Justice Perell, however, doubted that most of the settlement fund would be taken up by class members, given that there was little risk of identity theft and that there was no evidence that any class member had suffered a financial loss attributable to the breach.[93]

Although he ultimately approved the settlement, Justice Perell was clearly skeptical about the merits of the class proceeding. He cited the evidence of Home Depot's expert forensic investigator that:

> …despite utmost diligence and efforts to prevent data breaches, companies remain vulnerable because hackers continually develop new malicious code "and the game of cat and mouse continues." [The defendant's expert] deposed that the occurrence of a data breach is not proof of a lack of care and of not having taken appropriate preventative measures.[94]

In the court's view, "Home Depot was building a very strong case that it had done nothing wrong and there was mounting evidence that no Class Member had in fact been injured" and later described the plaintiffs' likelihood of success against Home Depot on the issues of both liability and damages as "negligible to remote."[95] Justice Perell also lauded Home Depot's response to a criminal breach of its computer systems as "responsible, prompt, generous, and exemplary."[96] He even went so far as to say that he would have approved a discontinuance of the class action with no compensation whatsoever to class members.[97]

While some of the Court's most critical comments on the strength of the plaintiffs' case were arguably obiter, they are a welcome signal that judges may apply more scrutiny to causes of action pleaded in privacy class actions going forward, focusing on the basic elements of liability (i.e. the defendant's conduct and the existence of compensable damages) rather than the mere existence of a data breach.

---

[89] *Lozanski v Home Depot Inc.*, 2016 ONSC 5447 at para 6.
[90] *Ibid* at paras 10-13.
[91] *Ibid* at paras 25, 48.
[92] *Ibid* at para 45.
[93] *Ibid* at paras 47-52
[94] *Ibid* at para 35.
[95] *Ibid* at paras 35, 74.
[96] *Ibid* at para 74
[97] *Ibid* at para 75.

7) Bennett v Lenovo (Canada) Inc

The plaintiff commenced a proposed national class action against Lenovo (Canada) Inc. ("Lenovo") and Superfish Inc., a software developer, alleging that an "adware program" called Visual Discovery was pre-installed onto certain Lenovo laptops.[98] As part of the operation of the software, certain information including the URL of the website being visited, the name of the merchant's website, the user's IP address and country, and session information was sent to Superfish's servers,[99] on an anonymous basis. The information was used only for the purpose of operating the software – to provide the user with information about other vendors selling the same product – potentially at a lower price (presumably a purpose that users had at least implicitly consented to by activating the software to find the product on other websites).

In the original version of the software installed on Lenovo's computers (before the updated version of the software was installed), there was a security vulnerability in the software, potentially allowing a third-party to gain access to the computer user's confidential and private information in limited circumstances.[100] There were no reports or evidence in Canada or elsewhere that the security vulnerability was exploited to access the private information of any user.[101]

The plaintiff alleged that the defendants were liable for (1) breach of the implied condition of merchantability; (2) the tort of intrusion upon seclusion; (3) breach of provincial privacy laws; (4) breach of contract; and (5) negligence.[102]

Prior to certification, Lenovo brought a motion to strike the plaintiff's claim in its entirety on the basis that it was plain and obvious that none of the causes of action advanced could succeed. The plaintiff subsequently withdrew his negligence claim.[103] At the motion to strike, Justice Belobaba of the Ontario Superior Court of Justice held that it was plain and obvious that the breach of contract claim would fail, on the basis that the alleged implied contractual term that the laptops would be free of any defects was contrary to the express provisions in the sales agreement, which provided that the software was being sold without warranties or conditions of any kind.[104] The Court found that it was not plain and obvious that the remaining three causes of action would fail.[105]

In finding that it is not plain and obvious that the claim for intrusion upon seclusion would fail, the Court reviewed the scope of *Jones.*[106] The plaintiff had pleaded that "the very act of implanting the software into the plaintiff's laptop was an intrusion upon the plaintiff's privacy", and that this conduct "exposed the class members to significant risks" – which the Court found satisfied the first two elements of the tort, recklessness and unlawful invasion.[107] The Court found that although the third element, distress, was not pleaded explicitly, it could be inferred from the content and tone of the pleading.[108] The Court further noted that the tort of intrusion

---

[98] *Bennett v Lenovo*, 2017 ONSC 1082 at para 3 [*Bennett* (Motion to Strike)].
[99] *Bennett v Lenovo (Canada) Inc*, 2017 ONSC 5853 at para 20 [*Bennett* (Certification)].
[100] *Ibid* at para 19.
[101] *Ibid* at para 28.
[102] *Bennett* (Motion to Strike), *supra* at para 7.
[103] *Bennett* (Certification), *supra* at para 32.
[104] *Bennett* (Motion to Strike), *supra* at para 32.
[105] *Ibid* at para 32.
[106] *Ibid* at paras 21-23, 27, 28.
[107] *Ibid* at paras 19-22.
[108] *Bennett* (Motion to Strike), *supra* at para 22.

upon seclusion was "just evolving. Its scope and content have not yet been fully determined."[109] Given the possibility of future growth for the tort, it was not plain and obvious that the claim would fail.[110]

With regard to the alleged breach of provincial privacy laws, Lenovo argued that there was no "pleading of any *actual* violation of anyone's privacy" nor any "allegation that any confidential information was actually hacked".[111] Therefore, Lenovo submitted that the statutory claims would be certain to fail.[112] The Court allowed the claims to proceed, but did so by making an analogy between Lenovo's unintended and initially unknown security vulnerability that had never been exploited and a deliberate act to facilitate a violation of physical privacy that had not yet been exploited:

> This Court has sensibly recognized an 'increased concern in our society about the risk of unauthorized access to an individual's personal information'. The risk of unauthorized *access* to private information is itself a concern even without any *actual* removal or actual theft. For example, if a landlord installs a peephole allowing him to look into a tenant's bathroom, the tenant would undoubtedly feel that her privacy had been invaded even if the peephole was not being used at any particular time. The same point can be made here.[113]

Emphasizing that the "scope and content of the provincial privacy laws in question [was] still evolving", Justice Belobaba found that the statutory privacy claims were not certain to fail.[114] There was no discussion in the decision of the potential chilling effect on innovation if unintended security vulnerabilities (which are constantly being discovered in software) could result in liability, particularly in the absence of actual damages.

Justice Perell subsequently certified the proceeding as a class action, but reformulated and narrowed the class definition and common issues.[115] The Court found that aggregate damages could not be certified as a common issue, because once liability questions were determined, the action must necessarily move on to the individual issues stage.[116] With respect to intrusion on seclusion, Justice Perell restated the common issues, so that they would focus on the specific elements that the Court of Appeal found in *Jones* would need to be established to make out a claim.

8) Conclusion

Five years after *Jones* was decided by the Ontario Court of Appeal, it has received surprisingly little meaningful consideration in Canadian jurisprudence. However, courts have appeared very willing to use intrusion upon seclusion as a springboard for the certification of privacy class

---

[109] *Ibid* at para 23.
[110] *Ibid* at para 23.
[111] *Ibid* at para 27 [emphasis in original].
[112] *Ibid*.
[113] *Ibid*.
[114] *Ibid* at paras 28-28.
[115] *Ibid* at paras 65, 68, 76.
[116] *Bennett (Certification)* at paras 79-80. But see *Daniells v McLellan*, 2017 ONSC 3466 at para 70, where the Court found that it was possible in that case to have an aggregate assessment of damages for intrusion upon exclusion.

actions, including by extending the tort to situations in which there is no deliberate conduct by the defendant and no "intrusion." Moreover, since *Jones v Tsige*, the courts have been willing to recognize new privacy-based causes of action, even in situations in which there is no gap in the existing law.

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 remedies 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. The more recent decisions in *Doe* and *Lozanski* suggest that they may meet with some resistance.

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 may leave companies vulnerable to what appears to be an expanding risk of class action litigation.