大成 DENTONS

A decade since the recognition of the tort of intrusion upon seclusion: How *Jones v Tsige* has impacted privacy class actions in Canada.

It has been ten years since the Ontario Court of Appeal first recognized the tort of intrusion upon seclusion in *Jones v Tsige*.[1] This paper discusses the impact of this decision on privacy class actions.

1. Recognition of the tort of intrusion upon seclusion

a. The facts in *Jones*

Jones and Tsige worked at different branches of a bank. Jones also maintained her primary bank account there. Jones and Tsige did not know or work with each other. However, Tsige became involved in a relationship with Jones' former husband. For about four years, Tsige used her workplace computer to access Jones' personal bank accounts at least 174 times. The information displayed included transactions details as well as personal information, such as date of birth, marital status and address. Tsige did not publish, distribute or record the information in any way.

Jones became suspicious that Tsige was accessing her account and complained to the bank. When the bank confronted Tsige, she admitted that she had looked at Jones' banking information, that she had no legitimate reason for viewing the information, and that she understood it was contrary to the bank's code of business conduct and ethics and her professional responsibility. Tsige explained then, and maintained throughout the litigation, that she was involved in a financial dispute with Jones' former husband and had accessed the accounts merely to confirm whether he was paying child support to Jones.

Jones sued for breach of privacy. The motion judge granted summary judgment and dismissed the claim for damages, holding that Ontario did not recognize a cause of action for invasion of privacy. The matter came before the Court of Appeal, which allowed the appeal, and recognized the cause of action.

b. The Court of Appeal's decision in *Jones*

i. The American context

The Court of Appeal began its analysis by commenting on the 1960 article by the American jurist William L. Prosser, "Privacy". Prosser's article had, in turn, been informed by the seminal 1890 article by S.D. Warren and L.D. Brandeis, "The Right to Privacy". Warren and Brandeis had argued for the recognition of a right to privacy to meet problems posed by technological and social change such as "instantaneous photographs" and "newspaper enterprise", which in their view had invaded "the sacred precincts of private life." Building on Warren and Brandeis' work, Prosser had canvassed

1 2012 ONCA 32 [*Jones*].

hundreds of American cases to delineate a four-tort "catalogue", which included "Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs." The Court of Appeal noted that the *Restatement (Second) of Torts*[2] had adopted Prosser's catalogue, framing the tort of intrusion upon seclusion as:

> One who intentionally intrudes, physically or otherwise, upon the seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the invasion would be highly offensive to a reasonable person.[3]

ii. The Canadian and international context

The Court of Appeal considered Canadian jurisprudence and found that, at least, it had left open the possibility of a cause of action based on intrusion upon seclusion. The Court of Appeal specifically considered *Charter* jurisprudence and found that it had recognized an interest in "informational privacy." The Court of Appeal also pointed out that five provinces (i.e., British Columbia, Manitoba, Saskatchewan, Québec, and Newfoundland and Labrador) had enacted open-ended legislation establishing a limited right of action for invasion of privacy (despite not specifically defining what constituted an invasion of privacy). Finally, the Court of Appeal noted that courts in the UK, Australia and New Zealand (in addition to the USA) had recognized common law torts for breach of privacy.[4]

iii. The Court of Appeal recognizes the tort

In view of these developments, the Court of Appeal concluded that it was appropriate to confirm in Ontario the existence of a right of action for intrusion upon seclusion.[5]

Noting that the facts in the case before it "cried out for a remedy",[6] the Court held, like Warren and Brandeis a century earlier, that it was the common law's duty to respond to the breakneck pace of technological change:

> The internet and digital technology have brought an enormous change in the way we communicate and in our capacity to capture, store and retrieve information. As the facts of this case indicate, routinely kept electronic data bases render our most personal financial information vulnerable. Sensitive information as to our health is similarly available, as are records of the books we have borrowed or bought, the movies we have rented or downloaded, where we have shopped, where we have travelled, and the nature of our communications by cell phone, e-mail or text message.
>
> [...]
>
> Technological change poses a novel threat to a right of privacy that has been protected for hundreds of years by the common law under various guises and that, since 1982 and the Charter, has been recognized as a right that is integral to our social and political order.[7]

---

2 [*Restatement*].

3 *Jones* at paras 15-19.

4 *Jones* at paras 25-54, 61-65.

5 The Court focused only on intrusion upon seclusion as that was the only one of the four Prosser privacy torts before it. It did signal that on different facts, it might be willing to explore the creation of other "right of privacy" torts in appropriate cases. *Jones* at paras. 16-21.

6 *Jones* at para 69.

7 *Jones* at paras 67-68.

The Court of Appeal found that Tsige's actions had been "deliberate, prolonged and shocking", that any person in Jones' position would have been "profoundly disturbed" by Tsige's actions, and that Ontario's laws would be "sadly deficient" were Jones to have no legal remedy.[8]

iv. The Court of Appeal defines the Canadian tort [9]

In defining the elements necessary to establish the tort, the Court of Appeal essentially adopted the formulation from the *Restatement:*

- The defendant's conduct must be intentional (which may include recklessness);
- The defendant must have invaded, without lawful justification, the plaintiff's private affairs or concerns; and
- A reasonable person would regard the invasion as highly offensive causing distress, humiliation or anguish.[10]

Crucially – and opening the proverbial class action floodgates – the Court of Appeal expressly held that "proof of harm to a recognized economic interest is not an element of the cause of action" and that, "given the intangible nature of the interest protected", damages would ordinarily be measured by a "modest conventional sum." The Court went on to note that a claim for intrusion upon seclusion would arise "only for deliberate and significant invasions of personal privacy" and that claims from "individuals who are sensitive or unusually concerned about their privacy are excluded: it is only intrusions into matters such as one's financial or health records, sexual practices and orientation, employment, diary or private correspondence that, viewed objectively on the reasonable person standard, can be described as highly offensive."[11]

In the Court's view, based on previous academic literature, common law jurisprudence and relevant legislation, damages for intrusion upon seclusion were a species of symbolic or moral damages to be fixed in a maximum of CA$20,000.[12]

---

8 *Jones* at para 69.

9 While the decision in *Jones* was only binding in Ontario, the tort has been adopted in some provinces. In others, most notably B.C., ambiguity continues about the existence of the tort. Because the decision in *Jones* was not appealed to the Supreme Court of Canada, there is no single binding national case.

10 *Jones* at para 71.

11 *Jones* at para 72.

12 *Jones* at para 87.

2. Intrusion upon seclusion in class actions

Jones quickly spawned privacy class actions. Since 2012, no less than 32 class actions have advanced claims for intrusion upon seclusion. Excluding six decisions approving certification for the purposes of settlement or otherwise on consent, of the remaining 26 class actions, 15 have been certified to include the tort,[13] while 11 have not been certified.[14] Interestingly, six of the 11 dismissals occurred just in the last year. The high water mark is clearly receding.

a. The initial tendency to certify

Courts initially embraced an openness to certifying claims for intrusion upon seclusion. This was for two main reasons. First, the threshold for certification is a low one under provincial class proceedings legislation.[15] With respect to the cause of action criterion, the test for whether a class proceeding discloses a cause of action is whether, assuming the facts as stated in the statement of claim can be proved, it is "plain and obvious" that the plaintiff's statement of claim discloses no reasonable cause of action.[16] The remaining four criteria require "some basis in fact", which imports a low evidentiary burden[17] and a standard that falls below the standard of proof on a balance of probabilities.[18] The less-than-onerous threshold for certification, in essence, precludes a court from meaningfully interrogating a plaintiff's claim. The result invariably tilts the scales towards certification.

Second, courts initially took the position that the tort was new and in need of development. For example, in the decisions in *Tucci*, *Casino Rama*, and *Agnew-Americano*, the courts indicated that the plaintiffs would likely encounter difficulty in ultimately proving that the defendants (who had had been victims of data breaches) had been "reckless", but certified the claims nonetheless. In each case, the courts relied on the fact that the tort of intrusion upon seclusion was still in development and in need of elaboration,[19] or otherwise unsettled.[20]

---

13 E.g. *Evans v Wilson,* 2014 ONSC 2135, leave to appeal ref'd, 2014 ONSC (Div Ct) (bank employee disseminating customer information to third parties). *Hynes v Western Regional Integrated Health Authority*, 2014 NLTD 137 (unauthorized employee access of personal health information). *Tucci v Peoples Trust Co.,* 2017 BCSC 1525, var'd 2020 BCCA 246 [*Tucci*]. *Daniells v McLellan*, 2017 ONSC 3466 (unauthorized employee access of personal health information). *MM v Family and Children's Services of Lanark Leeds and Grenville*, 2017 ONSC 7665 (dissemination of CAS records online). *Condon v Canada,* 2014 FC 250 (loss of external hard drive containing Student Program records). *Agnew-Americano v Equifax Co,* 2019 ONSC 7110 (data breach affecting defendant database) [*Agnew-Americano*]. *Tocco v Bell Mobility Inc.*, 2019 ONSC 2916 (use of customer personal information for marketing without consent.) *Severs v Hyp3R Inc.*, 2021 BCSC 2261 (defendant violated Instagram policy prohibiting 3rd parties from improperly collecting users' personal information and was removed from platform).

14 *Ladas v Apple Inc.,* 2014 BCSC 1821 [*Ladas*]. *Canada v John Doe,* 2015 FC 916, var'd 2016 FCA 191. *Broutzas v. Rouge Valley Health System*, 2018 ONSC 6315 [*Broutzas*]. *Kaplan v. Casino Rama Services Inc.*, 2019 ONSC 2025 [*Kaplan*]. *Simpson v. Facebook*, 2021 ONSC 968, aff'd 2022 ONSC 1284 [*Simpson*]. *Owsianik v. Equifax Canada Co.*, 2021 ONSC 4112 [*Owsianik*]. *Kish v. Facebook Canada Ltd.*, 2021 SKQB 198 [*Kish*]. *Del Giudice v. Thompson*, 2021 ONSC 5379 [*Del Giudice*]. *Obodo v Trans Union of Canada, Inc.,* 2021 ONSC 7297 [*Obodo*]. *Stewart v Demme,* 2022 ONSC 1790 [*Demme*]. *Winder v Marriott International Inc.,* 2022 ONSC 390 [*Winder*].

15 E.g. *Class Proceedings Act,* 1992, SO 1992, c 6.

16 *Hunt v Carey Canada Inc.,* [1990] 2 SCR 959 [Hunt].

17 *Fischer v IG Investment Management Ltd,* 2013 SCC 69 at para 40 [*Fischer*]. Pro-Sys Consultants Ltd. v Microsoft Corporation, 2013 SCC 57 at paras 102, 104 [*Pro-Sys*].

18 *Pro-Sys* at para 102.

19 *Tucci* at para 152, *Kaplan* at paras 28-29.

20 *Agnew-Americano* at para 135.

These two issues combined to initially create an environment in which there was no real substantive development in this area of the law.

b. Increasing skepticism

More recently, courts have begun to subject claims for intrusion upon seclusion to greater scrutiny.

i. Insufficiency of evidence

Some courts have begun to exercise a gatekeeping function to weed out unmeritorious claims early, applying the "some basis in fact" threshold. The decisions in *Simpson* and *Kish* illustrate this trend. Both lawsuits related to essentially identical allegations that the data brokerage Cambridge Analytica had obtained information about Canadian users of a social media company from a third-party application developer.

In *Simpson,* Ontario's Superior Court found that there was no evidence in the record that any Canadian users' personal data had been shared with Cambridge Analytica. The plaintiff's evidence was limited to:

- A notification from the social media company that the third-party application developer may have misused users' information;
- A report of the Office of the Privacy Commissioner commenting that there was no assurance that Canadians' personal information was not shared with Cambridge Analytica; and
- A public apology issued by senior officials of the social media company before Congressional and Parliamentary committees.[21]

Given the dearth of evidence, the Court found that there was no basis for the proposed common issues, and denied certification.[22] On appeal, the Divisional Court, citing its own decision in *Williams v Canon Canada Inc.,* held that it was the court's duty to screen out "abusive" or "unmeritorious fishing expeditions" and to consider whether a claim raised the "legitimate possibility" that the proposed common issues could be answered in the plaintiff's favour.[23] In light of its perceived role, the Court upheld the denial of certification.

In *Kish,* the Court of Queen's Bench for Saskatchewan noted that the plaintiffs were attempting to bolster the "barren" evidence from *Simpson* with expert evidence, as well as additional evidence from the plaintiff; neither of which the Court found admissible. This was because the plaintiff's affidavits consisted of various online news articles, government documents or reports, other class action complaints, academic articles and social media content , some of which she admitted to not even having read.[24] The Court found the expert's evidence to be defective because it did not establish his qualifications.[25] Having found the plaintiff's evidence inadmissible, the Court then found no evidentiary basis for the proposed common issues.

The decisions in *Simpson* and *Kish* were followed in *Chow v Facebook,*[26] which dealt with a claim alleging that the defendant had scraped users' call and text data without their knowledge or consent. While the claim in *Chow* was based on the BC *Privacy Act* (and not intrusion upon seclusion), BC's Supreme Court nonetheless cited *Kish* and *Simpson* for the proposition that it should exercise its gatekeeping function. As in those decisions, the Court noted that the plaintiff's evidence consisted of materials available online. The Court accepted the defendant's submission that the plaintiff's claim had essentially been "downloaded from the internet" and denied certification.[27]

---

21 *Simpson* at para 27.

22 *Simpson* at paras 44-45.

23 *Simpson* at para 27, citing *Williams v Canon Canada Inc.*, 2012 ONSC 3692 at para 23.

24 *Kish* at paras 50-52.

25 *Kish* at para 43.

26 2022 BCSC 137 [*Chow*].

27 *Chow* at para 39.

These decisions illustrate the increasing skepticism of courts towards evidence advanced by plaintiffs in support of claims for intrusion upon seclusion. However, they are based on the quality of plaintiffs' evidence, and do not elaborate on the doctrine itself. They also find courts wading dangerously close to assessing the merits of claims at certification. It remains to be seen whether the courts will continue to exercise their "gatekeeping" function where plaintiffs' evidence is not so obviously deficient.

ii. Database defendants

Courts have also begun to find that a defendant that is itself the victim of a cyberattack or other form of breach, a so-called "database defendant", cannot be said to be "intruding" the seclusion of class members.

In *Owsiniak,* the plaintiff's claim related to a breach of the defendant's systems that affected thousands of customers. Citing the Supreme Court of Canada in *Atlantic Lottery Corp. Inc. v Babstock,* Ontario's Superior Court held that "novel claims that are doomed to fail should be disposed of at an early stage and that courts can do so even if this requires resolving complex questions of law and policy."[28] The Court went on to find that extending liability to a person who does not intrude, but fails to prevent the intrusion of another, would be an unwelcome expansion of the tort.[29]

Following *Owsiniak,* Ontario's Superior Court in *Del Giudice* declined to certify a claim for intrusion upon seclusion against a company and its data hosting provider, both of which suffered a data breach. Further, the Court found that a "failure to prevent an intrusion, even a reckless failure to prevent, is not an intrusion" and that the defendants' failure to prevent the breach did not satisfy the third element of the test for intrusion upon seclusion.[30]

More recently, in *Winder,* Ontario's Superior Court considered a motion to strike the plaintiff's claim for failing to plead a legally viable cause of action. Again, the defendant had been the victim of a hacker and customer information was alleged to have been compromised as a result. The plaintiff argued that the defendant had obtained the class members' personal information on false pretenses, thereby rendering itself a reckless intruder that exposed stored personal information to the risk of being hacked. The Court rejected this argument, finding that the letter and spirit of the *Jones* court's decision prescribed a narrow ambit for the tort. Second, the Court found there was no need to the extend liability to defendants who obtained information by false pretenses, by breaching contractual promises or failing to comply with statutorily imposed privacy safeguards. Moreover, the Court found itself bound by the decisions in *Owsianik, Del Giudice* and *Obodo*.

These decisions make it clear that, moving forward, the tort of intrusion will likely be unavailable in class action claims against database defendants, although appellate clarification may still be needed. This would be in our view consistent with the test articulated in *Jones*.

28 *Owsianik* at para 53.

29 *Owsianik* at para 55. The decision in *Owsianik* was followed in *Obodo*.

30 *Del Giudice* at para 136.

iii. Nature of the intrusion

Courts have shown a willingness to deny certification based on the type of information affected.

For example, in *Broutzas,* the Ontario Superior Court did not certify a claim of intrusion upon seclusion arising from rogue employees' disclosure of the names and phone numbers of mothers who had given birth at the defendant hospital to RESP brokers, who later contacted the mothers using the information. As the breach was restricted to otherwise publicly available contact information, it did not intrude upon the class members' private affairs since "there is no privacy in information in the public domain, and there is no reasonable expectation in contact information, which is in the public domain, being a private matter." The breach was thus not highly offensive to a reasonable person causing distress, humiliation, and anguish.[31]

The Ontario Divisional Court in *Demme* went one step further. The defendant, Demme, had been employed as a nurse by the defendant hospital from 2007 to 2016. During that time, she stole nearly 24,000 opioid pills from the hospital's automated dispensing unit (ADU), before being caught (and having her employment terminated). In order to obtain the drugs, she had accessed the individual records of 11,358 patients, some of whom were in her circle of care.

For patients who were not in her circle of care, Demme had randomly selected patient names from the ADU display, giving her access to their name, ID number, the hospital unit they had visited, allergy information (if applicable), and any medication they had taken during the last 32 hours. This enabled Demme to discover which patients had taken opioids and have the ADU dispense medication to her for her own use. She only accessed each record for a matter of seconds, which was enough time to enable her to release the drugs. For patients who were in Demme's circle of care, she accessed their paper files in a similar manner.

On appeal, the Divisional Court examined the Court of Appeal's finding in *Jones* that there was no other remedy available for the plaintiff in that case to address the defendant's actions - i.e., the facts "cried out for a remedy." The Court held that this phrase informed the standard for what constitutes a "highly offensive" intrusion, and thus the tort should only be available in particularly serious instances.

The Court disagreed with the motions judge that "any intrusion – even a small one – into a realm as protected as private health information may be considered highly offensive." Here, Demme's access to patient records had been fleeting, the information accessed was not particularly sensitive, her motive had not been to obtain the information (but to obtain drugs), and there were no discernable effects on the patients. As a result, the Court held that the intrusion had not been highly offensive, even though it involved private health information. On this basis, the Court set aside the order certifying the action.

The Court's decision in *Demme* is helpful in that it recognizes that the manner or consequences of the alleged intrusion (and not simply the information affected) is relevant to the question of whether it was highly offensive. However, the emphasis on the "discernable effects" of Demme's activities on the patients (and whether their circumstances "cried out for a remedy") seems to invite a consideration of individual plaintiffs' circumstances. This would seem to import consideration of the effect of an intrusion on the claimant, which sits uneasily with the tort's recognition that it is protecting an intangible interest.

---

31 *Broutzas* at para 153. See also *Grossman v Nissan,* 2019 ONSC 6180 at para 10, where the court, in certifying intrusion upon seclusion as a cause of action, held that name, vehicle model and VIN, and vehicle lease or loan terms did not constitute "private information" but, for the purposes of certification, an individual's credit score could arguably be considered private information [*Grossman*].

This approach of assessing intrusion upon seclusion based on the privacy of the information is at odds with that taken by privacy regulators interpreting and enforcing Canada's personal information protection legislation. Under the latter approach, information – even if public (unless prescribed by statute) – is still "personal information", the loss of which may trigger reporting and notification obligations. Privacy regulators would likely find that, in the context of the unauthorized access here, even publicly available personal information could be considered sensitive. [32]

c. Subjective vs. Objective Criteria

The decision in *Demme* hints at a more fundamental problem with the notion of intrusion upon seclusion as a viable claim in class actions. This relates to both the second and third prongs of the test as formulated by the Court of Appeal – i.e., what constitutes the plaintiff's "private affairs or concerns" and what constitutes a "highly offensive" intrusion. These criteria necessarily invite, at least in part, a subjective assessment of the plaintiff's situation and, on that basis, are at odds with the "common issues" criterion.

With respect to the common issues criterion, the underlying question is whether allowing the claim to proceed as a class action will avoid duplication of fact-finding or legal analysis.[33] The focus is whether there are any issues the resolution of which would be necessary to resolve each class member's claim and which could be said to be a substantial ingredient of those claims.[34] The plaintiff must adduce some evidence that the common issue actually exists, and it can be determined on a class-wide basis.[35]

The requirement for a subjective assessment flows directly from the American authorities relied upon by the *Jones* court. As noted above, the Court of Appeal adopted the American formulation of the test found in the *Restatement*, which in turn had followed Professor Prosser's original formulation:

> Generally speaking, to make out cause of action for intrusion upon seclusion, a plaintiff must show (1) an unauthorized intrusion; (2) that the intrusion was highly offensive to the reasonable person; (3) the matter intruded upon was private; and (4) the intrusion caused anguish and suffering.[36]

The *Jones* court then considered American courts' approach to applying the test:

> With regard to the second element, factors to be considered in determining whether a particular action is highly offensive include the degree of intrusion, the context, conduct and circumstances of the intrusion, the tortfeasor's motives and objectives **and the expectations of those whose privacy is invaded**.[37] [Emphasis added]

32 Office of the Privacy Commissioner of Canada, 'Interpretation Bulletin: Sensitive Information' (May 2022).

33 *Western Canadian Shopping Centres Inc. v Dutton*, 2001 SCC 46 at para 39.

34 *Hollick v Toronto (City)*, 2001 SCC 68 at para 39.

35 *Kuiper v Cook*, 2020 ONSC 128 at paras 26-36; *Simpson* at para 43.

36 *Jones* at para 56.

37 *Jones* at para 58.

> In determining the third element, the plaintiff must establish that the expectation of seclusion or solitude was objectively reasonable. The courts have adopted the two-prong test used in the application of the Fourth Amendment of the United States Constitution. **The first step is demonstrating an actual subjective expectation of privacy**, and the second step asks if that expectation is objectively reasonable.[38] [Emphasis added]

It follows that an assessment of a claim for on intrusion upon seclusion requires the court to first consider whether the intrusion impacted an interest or matter that the plaintiff themselves in fact considered or expected to be private – a subjective test – and only then look at whether their subjective reaction (e.g., embarrassment or humiliation) was objectively reasonable in the circumstances. In the case of a class consisting of hundreds or thousands of individuals, this appears to be problematic.

However, thus far, Canadian courts have generally declined to accept this position. For example, the decision in *Grossman* dealt with a data breach affecting class members' credit scores. The defendants argued that the second element of the tort required individualized assessments, because every person's sensitivities about the release of their credit score would be different. The court disagreed, finding that the Court of Appeal's decision in *Jones* did not require any such analysis (emphasis in original).

I see no requirement for any such "subjective" analysis in the *Jones v Tsige* decision. To the contrary, the Court of Appeal made clear that it was adopting the formulation in the *American Restatement (Second) of Torts (2010),* a formulation that said nothing about subjective or individualized perspectives:

> One who intentionally intrudes, physically or otherwise, upon the seclusion of another or his private affairs or concerns, is subject to liability to the other for the invasion of his privacy, if the invasion would be highly offensive to a reasonable person.[20]

The Court of Appeal also made clear that subjective or individual "sensitivities" were not to be considered and that the determining norm was the objective assessment of the reasonable person:

> A claim for intrusion upon seclusion will arise only for deliberate and significant invasions of personal privacy. Claims from individuals who are sensitive or unusually concerned about their privacy are excluded: it is only intrusions into matters such as one's financial or health records, sexual practices and orientation, employment, diary or private correspondence that, viewed objectively on the reasonable person standard, can be described as highly offensive.[21]

I therefore conclude that the intrusion part of Common Issue No. 1 can be objectively answered on a class-wide basis through the lens of the reasonable person. [39]

Yet, there is some authority for the necessity of a subjective test. For example, the Ontario Superior Court's decision in *Kaplan* dealt with a cyberattack resulting in the personal information of its customers, employees and suppliers being stolen. The Court certified intrusion upon seclusion as a cause of action but declined to certify the proposed common issue based on intrusion upon seclusion:

---

38 *Jones* at para 59.

39 *Grossman* at paras 46-48.

> In this case, individual inquiries would be required to determine if class members were in fact embarrassed or humiliated by the disclosure of the fact that they were, for example, patrons of Casino Rama. Even if one or more of the representative plaintiffs could prove that she was embarrassed or humiliated, and that her reaction was objectively reasonable in the circumstances, no methodology has been provided to show how the individual assessments could translate into class-wide determinations.[40]

It is unclear why the reasoning in *Kaplan* has not been taken up. The decision there may rest on an unarticulated assumption that the necessity of individual inquiries only arises where a putative class is made up of different categories of individuals, for each of which a different type of information was intruded was upon. In cases where the class is composed of a single category of individual (e.g., customer), each of which has had the same information affected (e.g., credit score), the courts seem prepared to assume that all class members have the same expectation of privacy and would thus be impacted equally.

i. Compared with provincial *Privacy Act* jurisprudence

It is helpful to compare jurisprudence on the tort of intrusion upon seclusion with that of the statutory privacy torts, particularly the BC *Privacy Act*. It, as relevant, reads:

> *1 (1) It is a tort, actionable without proof of damage, for a person, wilfully and without a claim of right, to violate the privacy of another.*
>
> *(2) The nature and degree of privacy to which a person is entitled in a situation or in relation to a matter is that which is reasonable in the circumstances, giving due regard to the lawful interests of others.*
>
> *(3) In determining whether the act or conduct of a person is a violation of another's privacy, regard must be given to the nature, incidence and occasion of the act or conduct and to any domestic or other relationship between the parties.*

There is a line of authority in BC finding that s. 1(2) of the *Privacy Act* is incompatible with the common issues criterion. This culminated in the decision of the BC Supreme Court in *Chow*. There, the Court considered whether to certify common issues that essentially asked whether, by (i) collecting text and message data from its users (ii) without consent, (iii) the defendant social network had breached the *Privacy Act*. The court certified questions (i) and (ii), but declined to certify (iii) because there was no basis in fact that it could be resolved on a class-wide basis.

Considering the test under the *Privacy Act*, the Court noted that it must consider what is "reasonable in the circumstances"[41] and must have regard for the "nature, incidence and occasion of the act or conduct and to any domestic or other relationship between the parties."[42] The Court found that s. 1 requires consideration of the specific context in which an act or conduct occurs and the individual circumstances of the person claiming a breach, and thus imports subjective elements of reasonableness and context[43] that precluded it from being certified as a common issue.

---

40 *Kaplan* at para 80.

41 s. 1(2).

42 s. 1(3).

43 Citing *Ladas* at paras 179-183 and *Douez v. Facebook, Inc.*, 2014 BCSC 953 at para 283, rev'd but not on this point 2015 BCCA 279, rev'd but not on this point 2017 SCC 33; subsequent appeal from the BCSC judgment rev'd in part but not on this point 2018 BCCA 186, leave to appeal ref'd [2018] S.C.C.A. No. 298.

The tests under the *Privacy Act* and the tort of intrusion upon seclusion are clearly not identical. The former includes language that, on its face, requires a court to consider context. The latter does not, at least as currently interpreted by Canadian courts. However, it is submitted that proper interpretation of the tort of intrusion upon seclusion *does* require a contextual analysis that is fundamentally at odds with the common issues criterion.

Conclusion

It has now been 10 years since the Ontario Court of Appeal recognized the tort of intrusion upon seclusion. In the process, it opened a floodgate of class action litigation. However, we have increasingly seen the courts find ways to narrow the scope of the tort in class action proceedings. They have taken on a "gatekeeping" role, weeding out claims for which pleadings or evidence are clearly deficient. They have also determined that a defendant that is the victim of a third-party's actions is not itself an "intruder". However, the contours of the doctrine remain in flux, perhaps because it has not been fully tested outside the context of certification motions. It remains to be seen whether a claim for intrusion upon seclusion will be decided on the merits.

Authored by Michael (Mike) Schafler, FCIArb, QArb and Luca Lucarini