DENTONS

Twelve years since the recognition of the tort of intrusion upon seclusion: How *Jones v. Tsige* continues to impact privacy class actions in Canada

It has been 12 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 that 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* (which it slightly reformulated in 2022):

- The defendant must have invaded or intruded upon the plaintiff's private affairs or concerns without lawful excuse [the conduct requirement];
- The defendant's conduct which constitutes the intrusion or invasion must have been done intentionally or recklessly [the state of mind requirement]; and
- A reasonable person would regard the invasion of privacy as highly offensive, causing distress, humiliation or anguish [the consequence requirement].[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 *Owsianik v. Equifax Canada Co.*, 2022 ONCA 813 [Owsianik] at para 54.

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 41 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 35 class actions, 18 have been certified to include the tort[13] while 17 have not been certified.[14] Interestingly, 11 of the 17 refusals to certify occurred in the last two years. 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*[19], 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 nonetheless certified the claims. 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,[20] or otherwise unsettled.[21]

These two factors combined to initially create an environment in which many claims were certified. However, the paucity of any decisions on the merits of those claims led to little substantive development of the doctrine.

---

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 [*Tucci*], 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). *Tocco v Bell Mobility Inc.*, 2019 ONSC 2916 [*Tocco*] (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). *Welshman v Central Regional Health Authority*, 2024 NLSC 35 [*Welshman*] (improper access of personal documents by agency employee). Sweet v Canada, 2022 FC 1228 (data breach of Government of Canada online accounts by hackers; this certification was decided before *Owsianik*). *Farrell v Attorney General of Canada*, 2023 ONSC 1474 [*Farrell*] (correctional facility guards conducting strip searches on inmates).

14 *Ladas v Apple Inc.*, 2014 BCSC 182¬1 [*Ladas*]. *Canada v John Doe*, 2015 FC 916, var'd 2016 FCA 191. *Broutzas v. Rouge Valley Health System*, 2018 ONSC 6315 [*Broutzas S.C.*], aff'd 2023 ONSC 540 [*Broutzas*]. *Kaplan v. Casino Rama Services Inc.*, 2019 ONSC 2025 [*Kaplan*]. *Simpson v. Facebook*, 2021 ONSC 968, aff'd 2022 ONSC 1284 [*Simpson*]. *Agnew-Americano v Equifax Co*, 2019 ONSC 7110 [*Agnew-Americano*], *rev'd Owsianik v. Equifax Canada Co.*, 2021 ONSC 4112, *aff'd Owsianik*, application for leave to appeal ref'd, 2023 CanLII 62019 (SCC). *Kish v. Facebook Canada Ltd.*, 2021 SKQB 198 [*Kish*]. *Del Giudice v Thompson*, 2021 ONSC 5379, aff'd 2024 ONCA 70 [*Del Giudice*]. *Obodo v Trans Union of Canada, Inc.*, 2021 ONSC 7297, aff'd 2022 ONCA 814 [*Obodo*]. *Stewart v Demme*, 2022 ONSC 1790 [*Demme*]. *Winder v Marriott International Inc.*, 2022 ONSC 390, aff'd 2022 ONCA 815, application for leave to appeal ref'd, 2023 CanLII 62025 (SCC) [*Winder*]. *Campbell v Capital One Financial Corporation*, 2022 BCSC 928 [*Campbell*]. *Carter v. LifeLabs Inc.*, 2023 ONSC 6104 (database defendant case denied certification following *Owsianik*). *Doan v Canada*, 2023 FC 968 [*Doan*]. *Highland Cannabis Inc. v Alcohol and Gaming Commission of Ontario*, 2024 ONSC 423.

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 For clarity, *Agnew-Americano* refers to the first instance decision in *Owsianik*. The style of cause changed because the original representative plaintiff was replaced by Alina Owsianik.

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

21 *Agnew-Americano* at para 135.

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 at the certification stage. The decisions in *Simpson, Kish* and *Doan* illustrate this trend. *Simpson* and *Kish* are 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 on 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.[22]

Given the dearth of evidence, the Court found that there was no basis in fact for the proposed common issues and denied certification.[23] 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.[24] In light of its self-declared gatekeeping 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 having read.[25] The Court also found the expert's evidence to be defective because it did not establish his qualifications.[26] Having found the plaintiff's evidence inadmissible, the Court held there to be no evidentiary basis for the proposed common issues.

The reasoning in *Simpson* and *Kish* was adopted in *Chow v. Facebook*,[27] which dealt with a claim alleging that the same social media company 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.[28]

In *Doan*, the representative plaintiff initiated a class proceeding against the RCMP in connection with its use of Clearview AI Inc.'s facial recognition services. The Federal Court of Canada found that Ms. Doan lacked an

22 *Simpson* at para 27
23 *Simpson* at paras 44-45.
24 *Simpson* at para 27, citing *Williams* v *Canon* Canada Inc., 2012 ONSC 3692 at para 23.
25 *Kish* at paras 50-52.
26 *Kish* at para 43.
27 2022 BCSC 137 [*Chow*]
28 *Chow* at para 39.

evidentiary basis for the identified common issues. The Court noted that several paragraphs of the representative plaintiff's affidavit were based on "unspecified media sources." Further, Ms. Doan admitted during her cross-examination that she was unfamiliar with some of the statements in her affidavit and that "she would have to consult her counsel in order to explain how she knew [these facts stated in these paragraphs] to be true."[29] The Court emphasized that Ms. Doan did not hold personal knowledge of all the facts she swore to and afforded the evidence she adduced less weight.[30] The Court cited *Simpson* in its discussion of the "some basis in fact" standard.[31]

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 meaningfully elaborate on the doctrine. Further, the *Simpson and Kish* decisions also found courts wading dangerously close to assessing the merits of claims at certification. In that regard, the recent decision of the BC Court of Appeal in *Situmorang v. Google, LLC* notably overturned what it determined to be an overly strict approach to gatekeeping taken by the lower court.[32] There, the plaintiffs alleged that the defendant had used facial recognition technology to extract, collect, store and use the facial biometric data of Canadians without their consent in order to further its own competitive advantage in the marketplace for photo-sharing and integration services. The certification judge found that the plaintiff's notice of civil claim to be "vague and speculative" and held that the plaintiffs had failed to adequately plead that the defendant had disclosed the face templates to third parties, or had used them for any purpose beyond providing users with the core feature of enabling them to search for and sort photos containing similar faces ("face grouping").

The Court of Appeal found that the certification judge had erred in expecting the plaintiffs to "plead with precision the use that the respondent has made of the data, or the extent to which it has permitted others to access the data" without the benefit of discovery and at the certification stage. The Court also noted that the certification judge had erroneously narrowed the plaintiffs' claim to the use of facial biometric data for the face grouping feature. The Court interpreted the notice of civil claim more broadly, stating:

> [T]he notice of civil claim pleads that the actionable misconduct is the respondent's undisclosed use of facial recognition technology to extract, collect, store, and use facial biometric data from users and non-users, and the issuance of public statements that were misleading about this practice. Whether the facial biometric data collected from class members was used, exclusively or otherwise, for the purpose of the face grouping function is, as the appellant argues, largely irrelevant to the viability of the pleaded causes of action.[33]

Finally, the Court also held that the certification judge had improperly engaged in an evidence-based assessment of the merits. Specifically, the Court found that the certification judge had made findings on contested issues of interpretation of several documents incorporated in the notice of civil claim (e.g., findings on the meaning of disputed language in the defendant's Terms of Service)

---

29 *Doan* at para 20.
30 *Doan* at para 186.
31 *Doan* at para 182.
32 2024 BCCA 9 [*Situmorang*].
33 *Situmorang* at para. 64.

ii. Database defendants

In Ontario, it is now settled law that a defendant that is 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 November 2022, the Court of Appeal for Ontario released its decisions in *Owsianik, Winder* and *Obodo* (**Database Defendant Trilogy**), where it concluded that the appellant class members did not have a viable cause of action in the tort of intrusion upon seclusion against the database defendants.

In *Owsianik*, the plaintiffs' intrusion upon seclusion claim related to a breach of the defendant's systems by third-party actors that impacted the sensitive financial information of thousands of customers. The plaintiffs alleged that the defendant's failure to take adequate steps to protect the plaintiffs from the intrusion upon their privacy by hackers constituted an intentional or reckless intrusion upon the plaintiffs' privacy. The Court of Appeal for Ontario dismissed the plaintiff's appeal and refused to certify the intrusion upon seclusion claim.

According to the Court, on the facts as pleaded, the defendant's conduct could not amount to an act of intrusion or invasion into the privacy of the plaintiffs. The intrusions alleged were committed by unknown third-party hackers, acting independently from, and to the detriment of, the interests of the defendant. There were no facts pleaded which could in law provide a basis upon which the actions of the hackers could be attributed to the defendants or that the defendants acted in consort with, or were vicariously liable for, the hackers' conduct. The Court also noted that the plaintiffs were not without remedy in the absence of the intrusion upon seclusion claim, as the defendant might have been liable for its failure to protect the plaintiffs' privacy interests in the stored material in negligence, contract and under various statutes. The Court's reasons in *Winder* and Obodo mirrored its reasoning in *Owsianik*.

Following *Owsianik*, the Court of Appeal in *Del Giudice* upheld a motion judge's decision to deny certification of a claim for intrusion upon seclusion against a company and its data hosting provider, both of which suffered a data breach. On appeal, the appellants (the class members) sought to distinguish their case from the Database Defendant Trilogy by arguing that the intrusion upon seclusion claim was based on the improper retention and misuse of data, including the improper aggregation and migration to a third-party platform.[34]

The Court of Appeal rejected this argument by pointing out that, regardless of whether the alleged misdeeds of the defendant and the third-party platforms are characterized as mistake in safeguarding information or improper retention and misuse, both characterizations fail to satisfy the "consequence requirement" of the tort of intrusion upon seclusion. In other words, the Court of Appeal found that the conduct – regardless of characterization – was not of a highly offensive nature causing distress, humiliation, or anguish to a reasonable person.[35]

Moving forward, the tort of intrusion upon seclusion will be unavailable in class action claims against database defendants, although the application of the tort of intrusion upon seclusion in database defendant cases may vary outside Ontario.

---

34 *Del Giudice* at para 33.

35 *Del Giudice* at para 35.

iii. Nature of the intrusion

Courts have increasingly shown a willingness to deny certification based on the intrusion or privacy invasion not being significant enough to warrant relief. For example, where an individual's informational privacy interest is at stake[36], the type of information affected combined with the context of the intrusion, informs the assessment of whether the intrusion is sufficiently significant. To date, Canadian courts have intertwined this analysis with their assessment of the "consequence requirement."

For example, in *Broutzas*, the Ontario Divisional Court upheld the Superior Court's denial of certification. The Superior Court had declined to 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 Registered Education Savings Plan 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.[37] The Divisional Court upheld the Superior Court's decision, noting that the motion judge was entitled to deference in his findings that the conduct did not amount to a "significant intrusion" into the plaintiffs' private affairs and that a reasonable person would not regard the intrusion as highly offensive.

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 that 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." Rather, the Court noted that 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.

---

36 *Jones*, in line with *Charter* s. 8 jurisprudence, recognized three types of privacy interests: personal privacy, territorial privacy, and informational privacy. Claims for tort of intrusion upon seclusion can be made if any of these three interests is impacted. The majority of privacy class actions that rely on the tort of intrusion upon seclusion engage information privacy interests. However, see *Farrell*, for an example of a decision certifying a claim in intrusion upon seclusion based the plaintiffs' personal privacy interest in their body.

37 Broutzas (S.C.) 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].

The Court's decision in *Demme* is illuminating 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.

The Divisional Court in *Broutzas* approved of the approach taken in Demme. The Court noted that the decision in *Demme* was in line with the Court of Appeal's decision in *Jones*, where Sharpe J.A. stated that claims should be limited to *significant* invasions of personal privacy, where "privacy intrusion is very serious."[38]

iv. Subjective vs. objective assessment

The decision in *Demme* hints at a more fundamental issue with the notion of intrusion upon seclusion as a viable claim in class actions. This relates to what constitutes the plaintiff's "private affairs or concerns" and what constitutes a "highly offensive" intrusion. These criteria would seem to 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. This is because 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.[39] 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.[40] The plaintiff must adduce some evidence that the common issue actually exists and it can be determined on a class-wide basis.[41]

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.[42]

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.**[43] [Emphasis added]
>
> 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.[44] [Emphasis added]

---

38 *Broutzas* at para. 40.

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

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

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

42 *Jones* at para 56.

43 *Jones* at para 58.

44 *Jones* at para 59.

It follows that an assessment of a claim for an 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 take 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.[45]

Yet, there is some authority for the necessity of a subjective test.[46] 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:

> 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.[47]

---

45 *Grossman* at paras 46-48.

46 See also *Broutzas* at para. 37, where the Divisional Court noted that the certification judge's decision was supported by the fact that "none of the representative plaintiffs subjectively alleged such a reaction", although the Court was keen to emphasize that this was not determinative of the issue.

47 *Kaplan* at para 80.

The reasoning in *Kaplan* has not been taken up. This decision 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., a customer), each of which has had the same information affected (e.g., a credit score), the courts seem prepared to assume that all class members have the same expectation of privacy and would thus be impacted equally.

More recently, the Ontario Court of Appeal's decisions in the Database Defendant Trilogy and *Del Giudice* reinforced a focus on the objective, rather than subjective, assessment of the "consequence requirement." In the Database Defendant Trilogy, the Court of Appeal reiterated that one of the three elements of the tort of intrusion upon seclusion is whether **a reasonable person** would view the intrusion as highly offensive. In *Del Giudice*, the Court of Appeal disposed of the intrusion upon seclusion claim on the basis that a reasonable person would not find the intrusion in that case highly offensive. There the plaintiffs' personal information was impacted by a data breach of the defendant's service provider. The plaintiffs attempted to distinguish their case from those in the Database Defendant Trilogy by pleading that the defendant had intruded in the plaintiffs' private affairs when it aggregated and sold financial information about the plaintiffs without their consent. The Court of Appeal noted, at para 35:

> [T]he aggregation and sale of the financial information obtained by [the defendant] … **is not highly offensive and could not be considered humiliating by a reasonable person.** Unlike genuine intrusion claims, there is nothing into which the [the defendant] can be said to have intruded. It solicited information and that information was given. The data was aggregated and inputted into algorithms to be used for marketing purposes. Nowhere, in any of this, is anything of an individual's biographical core exposed to public or private view. No individual is placed in a spotlight. [Emphasis added.]

The law thus appears to have moved decisively away from the reasoning in *Kaplan*. *Owsianik* specifically clarified that the "consequence requirement" seeks to answer the inquiry: "Would a **reasonable person** find the intrusion of privacy highly offensive, causing distress, humiliation or anguish?" This "reasonable person" standard does not shed the requirement of a contextual inquiry. However, it suggests that establishing the consequence element of the tort likely does not necessitate an individualized fact-finding process based on the subjective expectation of privacy of each member in a proposed class action. This direction remains at odds with the original formulation of the tort in the *Restatement* and, as discussed below, is incongruent with much of the jurisprudence under the statutory privacy torts.

v. 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. *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"[48] 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."[49] 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 that precluded it from being certified as a common issue.[50]

The tests under the *Privacy Act* and the tort of intrusion upon seclusion are obviously not identical. However, both call for a contextual analysis. Unlike their counterparts assessing claims under the *Privacy Act*, courts assessing claims for intrusion upon seclusion generally have been unwilling to treat class members' subjective expectations as a bar to satisfying the common issues criterion. It is submitted that, at least in some cases, the proper interpretation of the tort of intrusion upon seclusion does require courts to examine whether conducting a contextual analysis of the privacy invasion is feasible on a class-wide basis or whether the circumstances of the proposed class members are sufficiently unique to require individual assessment.

c. Recent developments

i. Class actions alleging misuse of personal information

Some recent class actions allege defendants' use of personal information without consent or legal authority. This type of scenario stands in contrast to the majority of the class actions discussed in this paper, which consist of allegations of unauthorized access by defendants, their employees or third party hackers. To date, *Tocco* is the only successful certification decision this category that includes an intrusion upon seclusion claim. In *Tocco*, the plaintiffs alleged that the defendant had used the personal information of its data service customers for its own marketing initiative without their consent. The application of intrusion upon seclusion to *Tocco* does not appear to have been a matter of contention at the certification stage.[51] *Tocco* has not yet been heard on the merits.

Del Giudice, where the defendant allegedly retained, aggregated and input plaintiff's personal information into machine learning algorithms without consent, also considered a misuse argument rooted in the intrusion upon seclusion tort. The Court of Appeal did not reject the idea of conduct involving misuse of personal information grounding an intrusion upon seclusion claim. However, the Court noted: "Unlike genuine intrusion claims, there is nothing into which the [defendant] can be said to have intruded."[52] This statement suggests that claims based on misuse of personal information, rather than unauthorized collection or access, might ultimately face difficulty clearing the tort's "conduct requirement" on the merits. Ultimately, the Court disposed of the matter on the basis that a reasonable person would not have found the conduct to be highly offensive. As noted above, alleged misuse of personal information was also pleaded in *Situmorang*. There, the BC Court of Appeal accepted

48 s. 1(2).

49 s. 1(3).

50 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, subsequent decision not on this point, 2022 BCSC 914.

51 *Tocco* at paras 25-27.

52 *Del Giudice* at para. 35.

that the plaintiffs' pleading that the defendant had extracted, collected and retained facial biometric data without consent satisfied the cause of action criterion.

Importantly, all three of the claims canvassed here alleged misuse **in addition to** improper collection or access. Grounding a claim for intrusion upon seclusion exclusively on the improper use of private information, rather than in addition to the improper collection of, or access to, that information, may not meet the conduct requirement of the tort; but the fact of misuse may well inform the significance of the privacy invasion. This remains an area to watch moving forward.

ii. The tort of intrusion upon seclusion in provinces with statutory privacy torts

The existence of the tort of intrusion upon seclusion in provinces with statutory causes of action remains uncertain.

In BC, several decisions have grappled with the issue of whether the existence of the statutory privacy tort at s. 1(1) of the BC *Privacy Act* precludes the recognition of the common law tort of intrusion upon seclusion in the province. Despite some authority in BC that there is no common law cause of action for breach of privacy in that province, the BC Court of Appeal commented in *Tucci* that it may be time to revisit the issue, but that ultimately the issue was not before the Court.[53] In *Situmorang*, the BC Court of Appeal similarly raised the possibility that there may be a common law tort of intrusion upon seclusion available in that province. However, as the issue was not addressed by the parties, the Court left the issue to be decided by the BC Supreme Court on remittal.[54]

The BC Court of Appeal made a similar observation in *Ari*, noting that the issue of whether or not there is a common law tort of breach of privacy in BC is "unsettled".[55]

In *Welshman*, a recent certification decision at the Supreme Court of Newfoundland and Labrador, the Court found that the existence of the statutory privacy tort[56] did not inhibit the development of the common law tort of intrusion upon seclusion.[57] Notably, the Newfoundland & Labrador *Privacy Act* explicitly states that the statutory privacy tort established in the Act is in addition to, and not in derogation of, rights of action or remedies available elsewhere.[58]

---

53 *Tucci* at paras. 53-68.

54 *Situmorang* at paras. 86-89.

55 2023 BCCA 331 at para. 69. Note, however, that in another certification decision, the plaintiff abandoned the intrusion upon seclusion claim based on the understanding that the common law tort does not exist in BC: see *K.W. v Accor Management Canada Inc.*, 2023 BCSC 1149 at para 36. In *Campbell*, at para 100, the BC Supreme Court relied on the certification decision in *Tucci BCSC* to deny certification of the intrusion upon seclusion claim and did not place much weight on the comments in *Tucci BCCA* that the existence of the tort of intrusion upon seclusion was unsettled in BC.

56 *Privacy Act*, RSNL 1990, c P-2, s. 3 [Newfoundland & Labrador Privacy Act].

57 *Welshman* at paras 31-40.

58 Newfoundland and Labrador *Privacy Act*, s. 7(1).

3. Conclusion

It has now been 12 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, albeit one that has recently been tempered in BC. The courts have also determined that a defendant that is the victim of a third-party's actions is not itself an "intruder". Finally, claims are now evolving past data incidents to also address alleged misuse of private information. Ultimately, 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, Luca Lucarini and Ana Qarri.

CSBrand-145207-Privacy undone series - intrusion upon seclusion-03 — 31/05/2024