COURT OF APPEAL FOR ONTARIO

CITATION: Owsianik v. Equifax Canada Co., 2022 ONCA 813
DATE: 20221125
DOCKET: C69995

Doherty, Tulloch and Miller JJ.A.

BETWEEN

Alina Owsianik

Plaintiff/Respondent (Appellant)

and

Equifax Canada Co. and Equifax Inc.

Defendants/Appellants (Respondents)

Jean-Marc Leclerc, Tassia Poynter and Adil Abdulla, for the appellant

Laura F. Cooper, Alex D. Cameron, Sarah J. Armstrong, Vera Toppings and Pavel Sergeyev, for the respondents

Heard: June 7, 2022

On appeal from the order of the Divisional Court (Associate Chief Justice Faye E. McWatt, Justice James A. Ramsay, and Justice Harriet E. Sachs, dissenting), dated June 9, 2021, with reasons reported at 2021 ONSC 4112, 18 B.L.R. (6th) 78 (Div. Ct.), allowing an appeal from the order of Justice Benjamin T. Glustein of the Superior Court of Justice, dated December 13, 2019, with reasons reported at 2019 ONSC 7110.

Doherty J.A.:

I

OVERVIEW

[1] In *Jones v. Tsige*, 2012 ONCA 32, 108 O.R. (3d) 241, this court recognized the tort of intrusion upon seclusion. In that case, the defendant repeatedly accessed the private banking records of the plaintiff, the former wife of the defendant's common-law partner, without lawful justification. Sharpe J.A., for the court, held that an intentional or reckless invasion of the private affairs of another, without lawful justification, in circumstances in which a reasonable person would regard the invasion as highly offensive and causing distress, humiliation or anguish, was actionable without proof of any pecuniary loss: *Jones*, at paras. 70-71.

[2] In June 2022, this court heard three grouped appeals, including this one, arising out of three separate class actions. In each of those proceedings, the plaintiffs sought to apply the tort of intrusion upon seclusion, first recognized in *Jones*, to defendants who, for commercial purposes, collected and stored the personal information of others ("Database Defendants"), and whose failure to take adequate steps to protect that information allowed third-party "hackers" to access and/or use the personal information.

[3] All three proceedings are at the certification stage. In each case, the Database Defendants argued that the intrusion upon seclusion claim should not

be certified because, as pleaded, it did not disclose a cause of action as required by s. 5(1)(a) of the *Class Proceedings Act, 1992*, S.O. 1992, c. 6. The Database Defendants submitted that the tort as defined in *Jones* targeted those who, like the defendant in *Jones*, had actually invaded or intruded upon the privacy of a plaintiff, by accessing that plaintiff's private information. The tort could not reach Database Defendants whose inadequate security measures may have allowed others, with no connection to the Database Defendants, to access the private information stored in the databases. The Database Defendants submitted that, just as the negligent operator of a storage facility does not become a thief when a third party takes advantage of the operator's negligence, enters a storage unit and steals property kept in that unit, the Database Defendants do not invade the privacy of the persons whose information is stored in the databases if a third party takes advantage of the Database Defendants' failure to adequately protect the information and accesses that information.

[4] In this proceeding, Ms. Owsianik, on behalf of the identified class, was initially successful in certifying an intrusion upon seclusion claim as part of a class proceeding. However, the majority of the Divisional Court reversed the motion judge and held the tort had no application to a Database Defendant when the private information was accessed by a third-party hacker acting independently of the Database Defendant. Sachs J., in dissent, would have upheld the motion

judge's decision to certify the intrusion upon seclusion claim. Ms. Owsianik appeals with leave of this court.

[5] In *Obodo v. Trans Union of Canada, Inc.*, 2021 ONSC 7297, heard with this appeal, Mr. Obodo, on behalf of the identified class, unsuccessfully brought a motion for an order certifying an intrusion upon seclusion claim against the Database Defendant, Trans Union of Canada, Inc. ("Trans Union"). The motion judge did, however, certify other common issues. Mr. Obodo appeals from the refusal to certify the intrusion upon seclusion claim.

[6] In *Winder v. Marriott International, Inc.*, 2022 ONSC 390, the other case heard with this appeal, Mr. Winder, on behalf of the identified class, brought a pretrial motion under r. 21.01(1)(a) of the *Rules of Civil Procedure*, R.R.O. 1990, Reg. 194, for a determination of a question of law. Mr. Winder asked the court to determine whether he had pleaded a legally viable cause of action for intrusion upon seclusion against Marriott and the related defendants ("Marriott"). Mr. Winder's claim alleged, among other things, that Marriott had failed to take adequate steps to protect the private information provided to it by Mr. Winder and others from being accessed and/or used by third-party hackers. The motion judge held that the claim as pleaded did not disclose a viable cause of action against Marriott for intrusion upon seclusion. The other claims made against Marriott were not in issue on the motion. Mr. Winder appeals from the motion judge's determination.

[7] I would dismiss all three appeals. On the facts as pleaded, the defendants did not do anything that could constitute 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 Database Defendants. There are no facts pleaded which could in law provide a basis upon which the actions of the hackers could be attributed to the Database Defendants. There are no material facts pled which indicate that the Database Defendants acted in consort with, or were vicariously liable for, the hackers' conduct. The identity of the hackers is unknown.

[8] On the claims as pleaded, the Database Defendants' fault lies in their failure to take adequate steps to protect the plaintiffs from the intrusion upon their privacy by hackers acting independently of the Database Defendants. As recognized in the courts below, the Database Defendants may be liable for their failure to protect the plaintiffs' privacy interests in the stored material in negligence, contract and under various statutes. The Database Defendants' failure to meet their common law duty of care, or their contractual and statutory responsibilities to the plaintiffs to properly store the data, cannot, however, be transformed by the actions of independent third-party hackers into an invasion by the Database Defendants of the plaintiffs' privacy.

II

THE APPROACH TO THE APPEALS

[9] The three appeals all turn on the application of the tort of intrusion upon seclusion to Database Defendants who have gathered and stored large amounts of personal information, and who allegedly, through their failure to properly secure the information, allowed intruders to access that information. The relevant facts are very similar in all three appeals. Many of the same arguments have been advanced and fully developed by counsel in all three appeals.

[10] I will address the issues and arguments common to all three appeals in the context of the *Owsianik* appeal. I do so because the reasons of the motion judge, and the reasons of the majority and dissenting judge in the Divisional Court, taken together, provide a comprehensive consideration of the issues. The reasons of the majority in the Divisional Court were also relied on by the motion judges in *Obodo*[1] and *Winder* to reject the intrusion upon seclusion claims advanced by the plaintiffs in those proceedings. To the extent that there are issues or arguments raised in *Obodo* or *Winder* that are not addressed in these reasons, I will consider them in the reasons directly applicable to those cases.

---

[1] The motion judge in *Obodo* was the same judge who had heard the certification motion in this case. In this case, he certified the intrusion upon seclusion claim. In *Obodo*, he declined to certify the claim, correctly holding that he was bound by the decision of the majority in the Divisional Court in this case.

III

THE RELEVANT ALLEGATIONS

[11] The proceedings are still at the certification stage. There are no findings of fact, only allegations. The factual allegations are, however, taken as true for the purposes of determining whether Ms. Owsianik has pleaded a proper cause of action for intrusion upon seclusion: *R. v. Imperial Tobacco Canada Ltd.*, 2011 SCC 42, [2011] 3 S.C.R. 45, at para. 22; *Bowman v. Ontario*, 2022 ONCA 477, 83 C.C.L.T. (4th) 235, at paras. 25, 38-41.

[12] There are many allegations advanced by Ms. Owsianik in the Amended Amended Statement of Claim ("Statement of Claim"). In addition to the intrusion upon seclusion claim, Ms. Owsianik successfully sought certification on other common issues relating to allegations of negligence, breach of contract, breach of consumer protection law, and breaches of privacy legislation enacted in several provinces. Apart from the intrusion upon seclusion claim, the other claims are not in issue on this appeal and I need not detail the allegations or the arguments for and against their viability. These reasons focus on the allegations relating to the intrusion upon seclusion claim.[2]

---

[2] For the purposes of the certification motion, the parties divided the proposed class into three groups. The intrusion upon seclusion claim applied to two of the three subclasses. Members of those two subclasses alleged their personal information held in Equifax's database had been accessed by third parties without legal justification.

[13] Equifax and related companies (referred to collectively as “Equifax”) operate around the world providing credit reporting services and credit protection services to customers. For the purposes of providing credit ratings to its customers, Equifax collects and aggregates financial and other information relating to millions of individuals and various corporate entities (“consumers”). The information gathered by Equifax is organized and analyzed by Equifax to assist its customers in assessing the credit worthiness of the consumers to whom the information relates. Those consumers do not give Equifax permission to accumulate or analyze the data, and have no control over Equifax’s collection of the data.

[14] In addition to providing credit ratings, Equifax also provided clients with services intended to protect those clients from fraud, identity theft, and other financial crimes. Equifax accumulated and stored information pertaining to those clients for the purposes of providing those services.

[15] Between mid-May and late July 2017, hackers gained unauthorized access to the personal information stored by Equifax. The information accessed included individuals’ social insurance numbers, names, dates of birth, addresses, driver’s licence numbers, credit card numbers, email addresses, and passwords.

[16] The data breach affected persons around the world. Equifax estimated that about 20,000 Canadians were affected by the breach.

[17] Equifax discovered that its data had been improperly accessed in July 2017. It made the breach public in September 2017.

[18] The Statement of Claim alleged that Equifax knew, because of the vast amounts of personal information held in its database, and the nature of that information, that it was a prime target for cybercriminals. Equifax acknowledged that the proper safeguarding of the information it held in its database was crucial to the services provided to its customers. Equifax represented, publicly and in its contract with clients, that it maintained strict security safeguards to prevent unauthorized access to, and use of, the private information Equifax had accumulated and aggregated.

[19] The Statement of Claim further alleged a litany of deficiencies in the security systems put in place by Equifax to protect access to the database. The allegations included:

- the defendants' cybersecurity was grossly inadequate and dangerously deficient;
- the defendants' data protection measures failed to meet the most basic industry standards;
- the defendants used outdated and obsolete software;
- the defendants used inadequate network monitoring practices;

- the defendants failed to restrict access to sensitive data to only those employees whose job responsibilities required such access; and
- the defendants failed to heed advice from external security experts warning of inadequacies in their cybersecurity, including calls to perform comprehensive system reviews.

[20] The Statement of Claim also alleged that Equifax was fully aware of the inadequacies in its system. Specific shortcomings were brought to Equifax's attention after security audits in 2014 and 2016.

[21] Ms. Owsianik further alleged that when Equifax became aware that its database had been improperly accessed, it failed to respond to the intrusion in a timely or effective manner.

[22] The Statement of Claim went on to describe the information accessed by the hackers as sensitive and comprehensive. The information could be used by fraudsters for a variety of criminal purposes, including identity theft.

[23] Ms. Owsianik pled that Equifax's failure to take appropriate steps to guard against unauthorized access to sensitive financial information in the database constituted an intentional or reckless intrusion upon her privacy. Paragraph 37 of the Statement of Claim sets out the intrusion upon seclusion claim:

> The actions of the defendants constitute intentional or reckless intrusions upon seclusion that would be highly offensive to a reasonable person, for which the defendants are liable. The defendants failed to take

> appropriate steps to guard against unauthorized access to sensitive financial information involving the Class Members' private affairs or concerns. Their actions were highly offensive, causing distress and anguish to Class Members, for which the defendants are liable and should pay damages. [Emphasis added.]

[24] The Statement of Claim sought pecuniary damages on several bases, general damages assessed in the aggregate, damages for the unlawful conduct of third-party hackers, including identity theft, and punitive damages.

IV

THE DECISIONS BELOW

[25] Equifax advanced several arguments on the certification motion against certifying the intrusion upon seclusion claim. The motion judge carefully dealt with each argument and rejected all of them: *Agnew-Americano v. Equifax Canada Co.*, 2019 ONSC 7110.[3]

[26] The Divisional Court granted Equifax leave to appeal on a single question of law:

> Did the motion judge err in finding that the tort of intrusion upon seclusion is available against collectors and custodians of private information, such as the defendants in this case, where the private information is improperly [accessed] by a third party, including in circumstances

[3] Ms. Owsianik is the "Jane Doe" referred to in the style of cause before it was amended. Subsequently, Ms. Agnew-Americano was removed as the proposed representative plaintiff and replaced by Ms. Owsianik.

> where the defendants are alleged to have acted recklessly?

[27] The order of the Divisional Court reflects the narrow basis on which it granted leave. The order struck only claims alleging an intrusion upon seclusion (i.e., paras. 3(iii), (iv) and (v) of the motion judge's order). The Divisional Court refused to consider claims not captured by the specific question on which leave had been granted: *Owsianik v. Equifax Canada Co.*, 2021 ONSC 4112, 18 B.L.R. (6th) 78 (Div. Ct.), at paras. 14-15. I take the same approach in these reasons.[4]

[28] The motion judge concluded, assuming the truth of the alleged facts, that it was not "plain and obvious" the intrusion upon seclusion claim could not succeed against Equifax. He stressed that a certification motion, and in particular a determination of whether the plaintiff had pleaded a cause of action, was not the forum in which to determine "what the law should be in novel circumstances or how unsettled existing law should be reconciled." If the law was not "fully settled", the case "must be permitted to proceed": *Agnew-Americano*, at paras. 79, 87-88.

[29] The motion judge carefully examined the reasons in *Jones* and considered the caselaw, some of which offered support for the availability of the claim against a Database Defendant. In reference to *Jones*, the motion judge said, at para. 133:

---

[4] As I would affirm the decision of the majority in the Divisional Court, that the intrusion upon seclusion claim does not disclose a cause of action, it is unnecessary for me to address the other arguments relevant to the intrusion upon seclusion claim considered by the motion judge. I also make no comment on the application of this analysis to the breach of privacy claims based on various provincial privacy statutes.

> The principles in *Jones* could apply to (or be expanded to include) a claim for intrusion upon seclusion against a Database Defendant arising from a hacker attack.

[30] The motion judge considered the meaning of the word "reckless" as used in *Jones* in describing the scope of a defendant's potential liability for acts of intrusion into the privacy of others. He noted that various meanings had been ascribed to the word in different legal contexts. In his view, it was not clear that the concept of recklessness could not capture the conduct alleged against Equifax in the claim: *Agnew-Americano*, at para. 160.

[31] In the Divisional Court, the majority, relying on *Atlantic Lottery Corp. Inc. v. Babstock*, 2020 SCC 19, 447 D.L.R. (4th) 543, held that novel legal claims which are doomed to fail even if the alleged facts are true, should be disposed of at the certification stage: *Owsianik*, at para. 53. The majority concluded the intrusion upon seclusion claim advanced by Ms. Owsianik fell within the "doomed to fail" category. Ms. Owsianik had not alleged that Equifax perpetrated any act capable of amounting to an intrusion or invasion of her privacy, but had instead alleged that Equifax failed to take appropriate steps to protect Ms. Owsianik from intrusions perpetrated by independent third-party hackers. In the majority's view, the pleadings mischaracterized Equifax's failure to protect Ms. Owsianik from the invasion of her privacy by third-party hackers, as an intrusion into Ms. Owsianik's privacy by Equifax. Ramsay J., writing for the majority, said, at para. 55:

> I agree with my colleague (paragraph 43) that Equifax's actions, if proven, amount to conduct that a reasonable person could find to be highly offensive. But no one says that Equifax intruded, and that is the central element of the tort. The intrusion need not be intentional; it can be reckless. But it still has to be an intrusion. It is the intrusion that has to be intentional or reckless and the intrusion that has to be highly offensive. Otherwise the tort assigns liability for a completely different category of conduct, a category that is adequately controlled by the tort of negligence. [Emphasis added.]

[32] In her dissent, Sachs J. concluded, at para. 36, that the analysis in *Babstock* had "little application to the case at bar." In her view, the "plain and obvious" test applied. The uncertainty in the caselaw and the relative novelty of the claim both spoke against disposing of the claim on a pretrial motion.

[33] Sachs J. was satisfied that the motion judge correctly interpreted *Jones*. The potential liability of a Database Defendant was not before the court in *Jones*, however, nothing in the judgment foreclosed an application of the intrusion upon seclusion tort to Database Defendants. In Sachs J.'s view, the references in *Jones*, both to the policies underlying the tort, and the need to provide an effective remedy to those whose privacy had been violated by persons gaining access to large databases could support the extension of the tort to negligent Database Defendants who recklessly allowed hackers to gain access to the information in their databases. She concluded, at para. 51:

> The tort is a new tort, whose limits have not been fully developed at common law in Canada. The rights at issue are fundamental rights that are facing unprecedented

> threats. The common law should be allowed to develop in an incremental way to see how far the tort should be extended to meet those threats.

V

ANALYSIS

(i) The test under s. 5(1)(a) of the *Class Proceedings Act, 1992*

[34] A court cannot certify a class proceeding unless the prerequisites to certification set down in s. 5(1) of the Act are met. Section 5(1)(a) requires:

> The pleadings or the notice of application discloses a cause of action.

[35] A determination that a plaintiff has or has not pled a cause of action for the purposes of s. 5(1)(a) raises a question of law alone, reviewable on a correctness standard: *Bowman*, at para. 26.

[36] Counsel for Ms. Owsianik submits that the requirement in s. 5(1)(a) that the claim "disclose a cause of action" sets a low bar and is not intended to pre-empt novel, or tenuous claims. On the motion, the court must read the pleadings generously, accept as true the facts as pleaded and determine whether, on those facts, it is "plain and obvious" that the plaintiff has no cause of action against the defendant: *Imperial Tobacco*, at para. 17; *Hunt v. Carey Canada Inc.*, [1990] 2 S.C.R. 959, at p. 980.

[37] The test to be applied in deciding whether a claim discloses a cause of action for the purposes of s. 5(1)(a) is the same as the test to be applied on a motion to

strike a pleading as disclosing no reasonable cause of action under r. 21.01(1)(b): *Babstock*, at para. 14. I accept that a claim should only be struck if it is "plain and obvious" that the claim cannot succeed. I also agree that *Babstock* has not altered that test.

[38] *Babstock* is, however, helpful in that it demonstrates the application of the "plain and obvious" criterion in circumstances in which novel legal claims are advanced by plaintiffs. In *Babstock*, the plaintiffs relied on the doctrine of waiver of tort in support of one of the claims advanced by them. The defendant moved to strike, claiming that the doctrine did not exist in Canadian law and therefore the cause of action based on the doctrine could not succeed.

[39] At the time of the motion to strike, no court had recognized the doctrine of waiver of tort. Several courts had, however, certified claims, relying on the doctrine after concluding it was not "plain and obvious" that those claims could not succeed: *Babstock*, at para. 15. There was some academic support for the doctrine, although it seems from the comments in *Babstock*, at para. 21, that the weight of that support is waning. It was also clear that the availability of the doctrine on the facts as pleaded raised a pure question of law in the sense that the answer to the question could not be affected by any evidence that might be adduced at the trial. As observed by Brown J., at para. 21:

> Nothing is gained, and much court time and considerable litigant resources are lost, by leaving this issue unresolved.

[40] Some of the factors in *Babstock* outlined above exist in this case. No decision has held that the tort of intrusion upon seclusion applies to Database Defendants based on negligent or reckless storage of private information. Such claims have been certified in class actions, but on the basis that it is not "plain and obvious" the claim cannot succeed: e.g., *Bennett v. Lenovo (Canada) Inc.*, 2017 ONSC 1082, at paras. 8, 17, 23 and 36; see also *Kaplan v. Casino Rama*, 2019 ONSC 2025, 145 O.R. (3d) 736, at paras. 28-29[5]; *Tucci v. Peoples Trust Company*, 2020 BCCA 246, 41 B.C.L.R. (6th) 250, at paras. 53-88, rev'g in part 2017 BCSC 1525. The legal viability of the intrusion upon seclusion claim is also amenable to determination based exclusively on the facts as pleaded. There is no reason to think evidence adduced at the trial would have any effect on the determination of whether, as a matter of law, the tort could apply to Database Defendants whose failure to properly protect the data permits independent hackers to access the data.

[41] In *Babstock*, at para. 19, Brown J. addressed the application of the "plain and obvious" criterion to a case in which a novel claim is advanced, the viability of which turned exclusively on the application of the law as determined on the motion to the facts as pled by the plaintiff:

---

[5] An appeal to this court in *Kaplan* was dismissed as abandoned.

> Of course, it is not determinative on a motion to strike that the law has not yet recognized the particular claim. The law is not static, and novel claims that might represent an incremental development in the law should be allowed to proceed to trial [citation omitted]. That said, a claim will not survive an application to strike simply because it is novel. It is beneficial, and indeed critical to the viability of civil justice and public access thereto that claims, *including novel claims*, which are doomed to fail be disposed of at an early stage in the proceedings. This is because such claims present "no legal justification for a protracted and expensive trial" [citation omitted]. If a court would not recognize a novel claim when the facts as pleaded are taken to be true, the claim is plainly doomed to fail and should be struck. In making this determination, it is not uncommon for courts to resolve complex questions of law and policy [citations omitted]. [Emphasis added.]

[42] I take the majority in *Babstock* to recognize that when the validity of a claim turns exclusively on the resolution of a legal question, the court may on a pleadings motion, even if the answer to the legal question is complex, policy-laden and open to some debate, determine the law and apply the law as determined to the facts as pleaded to decide whether "the claim is plainly doomed to fail and should be struck."

[43] *Babstock* is consistent with prior authority from the Supreme Court of Canada. In *Nelles v. Ontario*, [1989] 2 S.C.R. 170, the plaintiff sued the Crown and the Attorney General of Ontario for malicious prosecution. The defendants brought a pretrial motion to strike the claim on the basis that the Crown and the Attorney General enjoyed absolute immunity from a malicious prosecution lawsuit. The

motion judge and a unanimous Court of Appeal accepted that argument. The majority of the Supreme Court reversed, holding that, while the Crown was immune from prosecution, the Attorney General and his agents were not.

[44] Lamer J., for five of six judges, held, at pp. 176-77, that the immunity of the Crown and the Attorney General was properly determined on a pretrial motion, whether that motion was styled as a motion on a question of law or a motion to strike the claim as not revealing a cause of action. Lamer J. described the immunity issue as raising "a question of law that goes to the root of the action". In his view, a timely pretrial determination of the legal viability of the malicious prosecution claim against the Attorney General would expedite the proceedings and potentially save unnecessary costs.

[45] The question of the Attorney General's immunity from a malicious prosecution lawsuit could hardly be described as "fully settled" law at the time of the *Nelles* litigation. Five judges, including the motion judge, three judges of this court, and one judge of the Supreme Court of Canada, held the Attorney General had immunity. The five-person majority in the Supreme Court, however, held that the Attorney General did not enjoy immunity from a malicious prosecution lawsuit. As set out in the judgment of Lamer J., the law in other jurisdictions was also unclear and unsettled. Despite the contentious nature of the legal issue, the majority held that it could properly decide that issue on a pretrial pleadings motion. This same approach is reflected in the recent judgment of the Supreme Court of

Canada in *Ontario (Attorney General) v. Clark*, 2021 SCC 18, 456 D.L.R. (4th) 361. There, the court struck a misfeasance in public office claim on the basis that the tort could not be extended to a claim brought by police officers against Crown attorneys in respect of their conduct of a prosecution.

[46] As catalogued by Brown J. in *Babstock*, there are several advantages to determining the viability in law of a claim on a pleadings motion when that viability turns exclusively on a question of law and the only material facts relevant to the question are those pled by the plaintiff. Deciding those questions early in the litigation serves judicial efficiency, enhances access to justice, and promotes certainty in the law: *Babstock*, at paras. 18-21; see also *Arora v. Whirlpool Canada LP*, 2013 ONCA 657, 118 O.R. (3d) 113, at paras. 90-93, leave to appeal refused, [2013] S.C.C.A. No. 498; Stephen G.A. Pitel & Matthew B. Lerner, “Resolving Questions of Law: A Modern Approach to Rule 21” (2014) 43:3 Adv. Q. 344.

[47] The effect of leaving legal questions bearing on the viability of a claim unresolved while the claim proceeds through trial is evident from a review of the class action proceedings involving intrusion upon seclusion claims against Database Defendants. Several of those claims have been allowed to move forward, not on the basis that the intrusion upon seclusion claim could actually be made out against the Database Defendant, but rather on the basis that it was not “plain and obvious” the claim could not succeed. Those decisions leave the law unclear and the ultimate viability of the claim uncertain.

[48] Class proceeding actions in which an intrusion upon seclusion claim is made against Database Defendants have continued to enter the system and continued to be certified on the same basis up to the Divisional Court's decision in this case. As these cases have slowly wended their way through the system, consuming valuable litigation resources, no one could say with any certainty whether the cause of action asserted in these claims existed as a matter of law. That question would only be answered in the litigation if and when one of the claims actually made it through trial. If a claim actually got that far, the trial judge would be obligated to decide exactly the same legal question that was before the motion judge on the certification motion months, if not years, earlier. And yet the trial judge would be in no better position to resolve that question than the motion judge.

[49] Not only did allowing these cases to proceed to trial result in uncertainty, that uncertainty arguably resulted in unfairness to Database Defendants. The certification of intrusion upon seclusion claims without a determination that the claim was viable in law gave a plaintiff an advantage in certification proceedings. Because damages for intrusion upon seclusion do not require proof of any actual pecuniary loss, but are instead awarded on a "symbolic" or "moral" basis, damages are well suited to an award on a class-wide basis. The nature of the damages to be awarded offered support for the plaintiff's argument that a class proceeding was the preferable proceeding for the resolution of common issues: *Class Proceedings Act, 1992*, s. 5(1)(d). Consequently, the presence of an intrusion upon seclusion

claim, despite the uncertainty as to its legal viability, gave plaintiffs a leg up in the certification process and, as a result, in any settlement negotiations: see *Winder*, at para. 16; *Babstock*, at para. 21.

[50] I accept that there are legitimate arguments on both sides of the debate over the legal viability of the intrusion upon seclusion claim against Database Defendants. The parties did not refer to any appellate authority in Canada or elsewhere in the Commonwealth directly on point. However, uncertainty in the law did not require the motion judge to decline to resolve the legal question at the certification stage. Four factors offered strong justification for deciding the legal viability of this claim on the certification motion:

- the question fell to be answered on the facts as pleaded. There was no dispute as to the facts that were relevant and material to the legal viability of the cause of action pleaded. There was no chance any evidence could be led at trial that would impact on the answer to the legal question posed;
- there was no unfairness to either party in deciding the merits of the legal question on the pleadings motion;
- the issue was fully briefed and argued on the pleadings motion; and
- the institutional considerations articulated in *Babstock* favoured deciding the legal question on the merits.

[51] The majority in the Divisional Court properly determined whether the claim as pled could in law amount to an intrusion by Equifax into the privacy of the plaintiffs. The majority's finding that the facts could not amount in law to the required intrusion meant that it was "plain and obvious" the claim could not succeed and should be struck.

(ii) Can Equifax be liable for the tort of intrusion upon seclusion?

[52] Having concluded the majority in the Divisional Court properly addressed the legal viability of the intrusion upon seclusion claim, it remains for me to explain why I agree with the conclusion reached by the majority.

[53] The tort of intrusion upon seclusion is one of several intentional torts which, when taken together, provide "broad protection of the plaintiff's personal integrity and autonomy": Philip H. Osborne, *The Law of Torts*, 6th ed. (Toronto: Irwin Law, 2020), at p. 268. Generally speaking, intentional torts require that the defendant engage in the proscribed conduct with a specified state of mind.

[54] The elements of the tort of intrusion upon seclusion are laid down in *Jones*, at para. 71. I would describe them as follows:

- the defendant must have invaded or intruded upon the plaintiff's private affairs or concerns, without lawful excuse [the conduct requirement];
- the 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].

[55] In *Jones*, the conduct component of the tort was never in dispute. The defendant admitted that she had, without lawful excuse, taken advantage of her employment to look at the plaintiff's banking records and related information on 174 occasions. On any definition, the defendant's conduct amounted to a deliberate invasion by her of the plaintiff's personal privacy: *Jones*, at paras. 57, 72.

[56] The conduct component is very much in issue in this case. Equifax stored the data and accessed and used the data for commercial purposes. That is not, however, the conduct which is alleged to have constituted the interference with the plaintiffs' privacy. As set out above (at para. 23), the alleged intrusion occurred when:

> The defendants failed to take appropriate steps to guard against unauthorized access to sensitive financial information involving the Class Members' private affairs or concerns.

[57] On the allegation made, Equifax failed to take steps to prevent independent hackers from conduct that clearly invaded the plaintiffs' privacy interests in the documents stored by Equifax. Equifax did not, however, itself interfere with those privacy interests. The wrong done by Equifax arose out of Equifax's failure to meet

its obligations to the plaintiffs to protect their privacy interests. Like the majority in the Divisional Court, I conclude the claim fails at this fundamental level. There is simply no conduct capable of amounting to an intrusion into, or an invasion of, the plaintiff's privacy alleged against Equifax in the claim: *Owsianik*, at para. 55; see also *Del Giudice v. Thompson*, 2021 ONSC 5379, 71 E.T.R. (4th) 23, at paras. 137-38.

[58] Ms. Owsianik submits that her claim does allege an intrusion upon seclusion because she pleads that the defendant acted recklessly. *Jones* recognizes that recklessness will suffice to establish liability.

[59] Ms. Owsianik's submission misunderstands the relationship between the two elements of the tort. The first element, the conduct requirement, requires an act by the defendant which amounts to a deliberate intrusion upon, or invasion into, the plaintiffs' privacy. The prohibited state of mind, whether intention or recklessness, must exist when the defendant engages in the prohibited conduct. The state of mind must relate to the doing of the prohibited conduct. The defendant must either intend that the conduct which constitutes the intrusion will intrude upon the plaintiffs' privacy, or the defendant must be reckless that the conduct will have that effect. If the defendant does not engage in conduct that amounts to an invasion of privacy, the defendant's recklessness with respect to the consequences of some other conduct, for example the storage of the information, cannot fix the defendant with liability for invading the plaintiffs' privacy.

[60] Intention is established if the defendant meant to intrude upon the privacy of the plaintiff or knew that it was a substantially certain consequence of the act which constitutes the intrusion: see *Piresferreira v. Ayotte*, 2010 ONCA 384, 319 D.L.R. (4th) 665, at paras. 72-75, leave to appeal refused, [2010] S.C.C.A. No. 283. Recklessness, also a subjective state of mind, refers to the realization at the time the prohibited conduct is being done that there is a risk that the conduct will intrude upon the privacy of the plaintiffs, coupled with a determination to nonetheless proceed with that conduct: see *Demme v. Healthcare Insurance Reciprocal of Canada*, 2022 ONCA 503, 83 C.C.L.T. (4th) 1, at paras. 62-64. The degree of recklessness required to fix liability can vary and need not be addressed in these reasons.

[61] In summary, the claim brought against Equifax fails at the conduct component of the tort of intrusion upon seclusion. Equifax's negligent storage of the information cannot in law amount to an invasion of, or an intrusion upon, the plaintiffs' privacy interests in the information. Equifax's recklessness as to the consequences of its negligent storage cannot make Equifax liable for the intentional invasion of the plaintiffs' privacy committed by the independent third-party hacker. Equifax's liability, if any, lies in its breach of a duty owed to the plaintiffs, or its breach of contractual or statutory obligations.

[62] Counsel on behalf of Ms. Owsianik submits that the extension of the tort from the actual intruder to entities who fail to adequately protect information in their

possession is, like the recognition of the tort in *Jones*, an incremental development in the common law: *Jones*, at para. 65. Counsel contends that the development is fully justified, given the state of the law in other jurisdictions, the realities of modern technology, the threats to individual privacy posed by the accumulation of large amounts of private information, and the absence of any effective remedy for persons whose information held in databases is accessed and used improperly.

[63] I do not agree that extending liability for the commission of the intentional tort of invasion of privacy by a stranger to Equifax would amount to an incremental change in the law. The extension of the common law proposed in this submission would not be a small step along a well-established path, but would be a giant step in a very different direction: see *Merrifield v. Canada (Attorney General)*, 2019 ONCA 205, 145 O.R. (3d) 494, at paras. 20-26, leave to appeal refused, [2019] S.C.C.A. No. 174.

[64] On the alleged facts, Equifax did not unlawfully access any information. No one acting on Equifax's behalf, or in consort with Equifax, did so. No one for whom Equifax could be held vicariously liable accessed any private information. A third-party stranger to Equifax accessed the information.

[65] To impose liability on Equifax for the tortious conduct of the unknown hackers, as opposed to imposing liability on Equifax for its failure to prevent the hackers from accessing the information, would, in my view, create a new and

potentially very broad basis for a finding of liability for intentional torts. A defendant could be liable for any intentional tort committed by anyone, if the defendant owed a duty, under contract, tort, or perhaps under statute, to the plaintiff to protect the plaintiff from the conduct amounting to the intentional tort. The security guard who fell asleep on the job, recklessly allowing an assailant to assault the person who the security guard was obliged to protect, would become liable for battery. The garage operator who negligently, and with reckless disregard to the risk of theft, left the keys in a vehicle entrusted to his care, would become a thief if an opportunistic stranger stole the car from the garage parking lot.

[66] Not only would the scope of intentional torts expand, that expansion would radically reconfigure the border between the defendant's liability for the tortious conduct of third parties, and the defendant's direct liability for its own failure to properly secure the information of the plaintiffs. The distinction between the two forms of liability is made clear in *Fullowka v. Pinkerton's of Canada Ltd.*, 2010 SCC 5, [2010] 1 S.C.R. 132. In that case, the plaintiffs sued Pinkerton's (and others) who were responsible for mine safety during a violent strike. The plaintiffs alleged Pinkerton's had failed to protect the victims who were killed in a bombing caused by a striker. Cromwell J., for a unanimous court, explained the nature of Pinkerton's' potential liability, at paras. 16-17:

> The appellants do not allege that either Pinkerton's or the Government actually inflicted the fatal injuries on the murdered miners; rather, they allege that Pinkerton's and

> the government breached a duty to take reasonable care to prevent the harm inflicted by Mr. Warren [the bomber]. The Court of Appeal characterized this as a claim that Pinkerton's and the government were liable for Mr. Warren's tort (para. 98). This however is not the right way to frame the issue because it does not accurately reflect the appellants' claims.
>
> We are here concerned with allegations of direct liability. Simply put, the appellants do not claim that Pinkerton's and the government are responsible for Mr. Warren's tort; the claim is that they were negligent in trying to prevent it. The appellants' position is that primary liability should be imposed based on the fault of these two defendants [citation omitted]. The question is not, therefore, whether these defendants are responsible for the tort of another, but whether they, in relation to another's tort, failed to meet the standard of care imposed on them and thereby caused the ultimate harm. [Emphasis added.]

[67] The words of Cromwell J. ring true here. On a reading of the actual allegations in the Statement of Claim, the real complaint against Equifax is that it failed to guard the information it was duty-bound to protect.

[68] The law relating to a defendant's potential liability for the tortious conduct of "strangers" is well-developed in Canada and in England. That law will impose liability on Equifax if the plaintiff can show that Equifax had an obligation at tort, under contract, or perhaps under statute, to protect the private information stored in its database from access by third-party hackers, and failed to do so, thereby causing economic harm to the plaintiffs: see e.g., *Rankin (Rankin's Garage & Sales) v. J.J.*, 2018 SCC 19, [2018] 1 S.C.R. 587; *P. Perl (Exporters) Ltd. v. Camden London Borough Council*, [1983] EWCA Civ 9, [1984] Q.B. 342; and

Lewis N. Klar & Cameron Jefferies, *Tort Law*, 6th ed. (Toronto: Carswell, 2017), at pp. 598-604. The law as it exists properly fixes liability on the defendant for the defendant's misconduct and provides remedies consistent with the remedies available in contract and negligence for that kind of misconduct. I am not persuaded there are deficiencies in the present law calling out for the drastic change endorsed by the appellant.

[69] The appellant further argues that expanding the tort of intrusion upon seclusion the way she suggests is consistent with American caselaw. The parties in all three proceedings have referred to various American authorities said to support their respective positions on the expansion of the tort to include negligent Database Defendants.

[70] There can be no doubt that the American jurisprudence has long recognized the right to privacy as important and worthy of the protection of tort law. It is equally clear that the analysis in *Jones* was heavily influenced by American commentary. However, as is often the case, the sheer quantity of American caselaw and the different statutory provisions at play in many of the cases, make it difficult to arrive at any generalized conclusion about the state of the law.

[71] The cases relied on by the Database Defendants offer direct support for their position. Negligence cannot morph or be transformed into an intentional tort: see e.g., *Allgood v. Paperlesspay Corp.*, 2022 WL 846070 (M.D. Fla.); *Burton v.*

MAPCO Exp., Inc., 47 F. Supp. (3d) 1279 (N.D. Ala. 2014); *Stephens v. Availity*, 2019 WL 13041330 (M.D. Fla.); *Purvis v. Aveanna Healthcare, LLC*, 563 F. Supp. (3d) 1360 (N.D. Ga. 2021); and *Damner v. Facebook Inc.*, 2020 WL 7862706 (N.D. Cal.).

[72] In contrast, the cases relied on by the appellants do not directly support their position. This, to a large extent, is because the outcomes of those cases turn on other legal principles. Some cases are explained by vicarious liability: see e.g., *Savidge v. Pharm-Save, Inc.*, 2021 WL 3076786 (W.D. Ky.); *McKenzie v. Allconnect, Inc.*, 369 F. Supp. (3d) 810 (E.D. Ky. 2019); and *Carter v. Innisfree Hotel, Inc.*, 661 So. (2d) 1174 (Ala. 1995). Some cases are explained by statutory liability: see e.g., *In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, 846 F. (3d) 625 (3rd Cir. 2017). Some cases are explained by liability for other torts, like nuisance, trespass and negligence: see e.g., *Moore v. New York Elevated Railroad Co.*, 130 N.Y. 523 (1892); *Remijas v. Neiman Marcus Group, LLC*, 794 F. (3d) 688 (7th Cir. 2015).

[73] The American cases relied on by the appellants do affirm the importance of privacy rights and several of them affirm that a real injury can be suffered when there is a loss of privacy. The cases also make clear that a negligent actor can be held liable for reasonably foreseeable harms to which their actions give rise, including reasonably foreseeable intentional harms committed by independent third parties: see e.g., *Carter*; *Thetford v. City of Clanton*, 605 So. (2d) 835 (Ala.

1992). This, however, does nothing to support the view that negligent parties in this position should also be held liable for the intentional torts.

[74] In my view, the state of the American jurisprudence does not provide a justification for extending the tort to negligent database defendants.

[75] Ms. Owsianik submits that the remedies available against Equifax in a claim based on breach of contract, negligence, or breach of a statute, are inadequate. She contends that just as in *Jones*, she and her fellow victims are left in circumstances that "cry out for a remedy": *Jones*, at para. 69.

[76] In *Jones*, the plaintiff had no remedy of any kind against the defendant who had intentionally invaded her privacy. Ms. Owsianik and the other class members have a remedy against the hackers who intentionally invaded their privacy. They can sue for invasion of privacy. No doubt, they face a very real problem. In most cases it will be impossible to identify, much less sue, the hackers. The inability to sue the actual hackers is not, however, justification for creating a remedy against a different defendant who has committed a different tort for which the plaintiffs have all the usual remedies available to them. The inability to successfully sue the hacker is no reason to make a Database Defendant liable, not only for its own wrongdoing, but also for the invasion of privacy perpetrated by the hacker.

[77] To award "moral damages" against Equifax for what is essentially its negligence or breach of contract runs contrary to the very purposes underlying the

award of such damages. Moral damages are awarded to vindicate the rights infringed, and in recognition of the intentional harm caused by the defendant. These purposes are served only if the damages are awarded against the actual wrongdoer, that is the entity that invaded the privacy of the plaintiff.

[78] Ms. Owsianik and the other plaintiffs have remedies against Equifax. Those remedies are the same remedies available to anyone who can prove the claims advanced in tort, contract, and statute by the plaintiffs against Equifax.

[79] The plaintiffs' "no remedy" argument really comes down to the assertion that because the remedies available in contract and negligence require proof of pecuniary loss, the plaintiffs who cannot prove pecuniary loss are left with no remedy. With respect, this is not what the court meant in *Jones* when it described the plaintiff as being without remedy. The plaintiffs here are in the same position as anyone else who advances the kind of claim the plaintiffs have advanced here. Because the claim sounds in negligence and contract, the plaintiffs must prove pecuniary loss. The plaintiffs' position is miles away from the predicament faced by the plaintiff in *Jones*.

[80] While it cannot be said the plaintiffs are left without a remedy, it is true that the inability to claim moral damages may have a negative impact on the plaintiffs' ability to certify the claim as a class proceeding. In my view, that procedural

consequence does not constitute the absence of a remedy. Procedural advantages are not remedies.

[81] The plaintiffs have not made out the case for extending the tort of intrusion upon seclusion to Database Defendants whose negligent storage of information permits independent hackers to access that information. That is not to say that the risk to privacy presented by the accumulation of private information by Database Defendants is not real. It may be that existing common law remedies do not adequately encourage Database Defendants to take all reasonable steps to protect the private information under their control. Parliament and provincial legislatures have enacted legislation intended to protect informational privacy. It is certainly open to Parliament and the legislatures to expand these protections to provide for what Parliament and the legislatures might regard as more effective remedies against Database Defendants who do not take proper steps to secure the information under their control.

VI

CONCLUSION

[82] I would dismiss the appeal.

[83] I would award costs to Equifax in the amount of $25,000. That amount includes the costs of the leave application, disbursements and relevant taxes.

Released: “November 25, 2022 DD”

“Doherty J.A.”
“I agree. M. Tulloch J.A.”
“I agree. B.W. Miller J.A.”