THE LITIGATION CONSEQUENCES OF CYBER-SECURITY BREACHES – PART II

Ronald D. Davis, Alexander Evangelista, and Teodora Obradovic, Fogler Rubinoff LLP[*]

Table of Contents

Introduction to Part II: Common Law Remedies and Liability Avoidance

Part I of the Litigation Consequences of Cybersecurity Breaches ((2022), 53 Adv. Q. 127) introduced this audience to cyber threats and new attack vectors that threaten Canadians and organizations' cybersecurity. It explored Canada's statutory framework and its responses to the problems and harms caused by cyberattacks or cyberbreaches.

* The authors wish to acknowledge and thank their colleagues at Fogler, Rubinoff LLP, partner Bill Hearn and students-at-law John Jeyaratnam and Gideon Ampofo, for their assistance with this article.

There is no unitary statutory framework in Canada. Instead, there are several frameworks and regimes that attempt to address organizational cybersecurity obligations, as well as individual cybersecurity rights and protections. We reviewed these in Part I: Frameworks of General Application, such as *PIPEDA* or *FIPPA*, and sector-specific ones, such as the OSFI's guidelines for FRFIs, or IIROC's guidelines for dealer members.

Part I also looked forward hopefully to novel, robust cybersecurity legislation. But that hope remains distant relative to the cybersecurity protection Canadians expect from organizations.

As new threats or issues arise, courts continue in their efforts to expand the remedies and protections under those frameworks through thoughtful interpretation. However, these statutory frameworks are limited in the civil remedies they can offer for violations, and even more limited in the monetary redress they provide.

Enter the common law. In cybersecurity law's nascent state, cyberbreaches in Canada (and elsewhere) are accreting around privacy. This accretion is befitting. Privacy law is itself in a nascent state. It is in emerging privacy torts that most, if not all, cyberbreaches seek their civil litigation footing, in addition to repurposed existing torts (*e.g.*, negligence) or breach of contract.

Given these nascent states, our vista is limited. Just as there is no perfect technology or perfect technological solution to cyberbreaches, civil litigation as yet offers no single or perfect solution to cybersecurity issues.[1] Cyberbreach litigation is only beginning to take shape. Its *Donoghue v Stevenson* moment has yet to arrive. Part II of the Litigation Consequences to Cybersecurity Breaches will focus on (i) common law remedies, and (ii) some liability avoidance strategies.

Common Law Remedies: The Nexus Between Privacy and Cybersecurity

It is not possible to discuss the common law and cybersecurity without discussing the common law and privacy. The common law's approach to privacy and cybersecurity breaches is in its infancy. Canadian tort law's recognition of privacy has been fragmentary. U.S. tort law is far more developed. It has four established categories

1. Bryan P Schwartz et al, "Cybersecurity and Law Firms", *Asper Review of International Business and Trade Law*, Introduction, Volume 21 Special Edition – 2021 CanLIIDocs 988, https://canlii.ca/t/t58s, accessed July 9, 2022.

of privacy that give rise to common law actions: (a) intrusion upon seclusion; (b) appropriation of the other's name or likeness; (c) publicity given to another's private life; and (d) publicity that places another in a false light before the public.[2]

In Canada, invasions of privacy were originally thought to be a form of nuisance.[3] Slowly, Canadian courts have incrementally adopted parts of the American classification scheme as the foundation for privacy and cybersecurity litigation options.[4]

Yet, Canadian common law has no stand-alone tort of invasion, or breach, of privacy.[5] As noted in the preceding pages, some provinces – British Columbia, Manitoba, Newfoundland, and Saskatchewan – have enacted privacy legislation that creates the tort of violation of privacy, actionable without proof of damage.[6]

Privacy legislation in the common law provinces also includes the statutory tort of appropriation of personality. Manitoba, Newfoundland, and Saskatchewan group it as part of the general tort of violation of privacy. British Columbia includes it as a standalone tort.[7]

Other provinces – Alberta, Manitoba, Saskatchewan, Newfoundland, Prince Edward Island, and Nova Scotia – have introduced legislation creating a statutory tort for the non-consensual distribution of intimate images. A person who distributes another's intimate image will have committed a tort if they know there was no consent to the distribution or were reckless as to whether there was consent.[8]

2. William Prosser, "Privacy" (1960) 48 Cal L Rev 383; Restatement (Second) of the Law of Torts (1977), at 652A–E.
3. *Motherwell v. Motherwell* (1976), 73 D.L.R. (3d) 62, [1976] 6 W.W.R. 550, 1 A.R. 47 (Alta. C.A.).
4. *Broutzas v. Rouge Valley Health System*, 2018 ONSC 6315, 299 A.C.W.S. (3d) 469, 2018 CarswellOnt 17820 (Ont. S.C.J.) at para. 135, additional reasons 2019 ONSC 559, 303 A.C.W.S. (3d) 31, 2019 CarswellOnt 762 (Ont. S.C.J.), appeal quashed 2019 ONCA 751, 310 A.C.W.S. (3d) 700, 2019 CarswellOnt 15049 (Ont. C.A.).
5. *Broutzas, ibid*, at para. 133.
6. Tort of violation of privacy, actionable without proof of damage: *Privacy Act,* R.S.B.C. 1996, c. 373, s. 1*; Privacy Act*, C.C.S.M. c. P125, s. 2*; Privacy Act*, R.S.S. 1978, C. P-24, s. 2*; Privacy Act*, R.S.N.L. 1990, C. P-22, s. 3. Privacy torts are also protected under Québec legislation: *Charter of Human Rights and Freedoms,* C.Q.L.R. c. C 12, art.-5*; Civil Code of Québec*, C.Q.L.R. c. C.C.Q. 1991. art. 35.
7. *Privacy Act*, R.S.B.C. 1996, c. 373, s. 3; *Privacy Act*, C.C.S.M. c. P125, ss. 2-3; *Privacy-Act*, R.S.S. 1978, C. P-24, ss. 2-3; *Privacy Act*, R.S.N.L. 1990, C. P-22, ss. 3-4.
8. *Protecting Victims of Non-consensual Distribution of Intimate Images Act*, R.S.A. 2017, c P-26.9, s. 3; *The Intimate Image Protection Act*, C.C.S.M. c.

In provinces lacking privacy legislation, a person seeking remedies for a breach of their privacy rights must fit themselves into an existing common law cause of action. There is no dispute that existing privacy legislation does not occupy the field or displace the common law right to proceed with privacy claims.[9]

What appears to be clear is that wherever the common law goes with privacy, cybersecurity and its litigation consequences will follow.[10]

A. The Most Obvious Choice: Intrusion Upon Seclusion

The door to a cause of action for privacy breaches was first opened by the Court of Appeal for Ontario's recognition of the tort of intrusion upon seclusion in *Jones v. Tsige*.[11]

Ms. Jones and Ms. Tsige were both employed by the Bank of Montreal. Ms. Tsige also had a common law relationship with Ms. Jones' former husband. Ms. Tsige reviewed Ms. Jones' banking records at least 174 times. While Ms. Tsige did not publish or record the information in the records – it included Ms. Jones' date of birth, marital status, address, and transaction details – she admitted to reviewing them to confirm whether her common law husband was paying Ms. Jones child support.[12]

I87, s. 11; *Privacy Act*, R.S.S. 1978, C. P-24, s. 7.3; *Intimate Images Protection Act*, R.S.P.E.I. 1988, c. I-9.1, s. 3; *Intimate Images Protection Act*, R.S.N.L. 2018, c. I-22, s. 4; *Intimate Images and Cyber-protection Act*, S.N.S. 2017, c. 7, s. 5.

9. *Hopkins v. Kay*, 2014 ONSC 321, 119 O.R. (3d) 251, 237 A.C.W.S. (3d) 362 (Ont. S.C.J.) at paras. 29, 30, motion to quash dismissed 2014 ONCA 514, 249 A.C.W.S. (3d) 745, 2014 CarswellOnt 18886 (Ont. C.A.), affirmed 2015 ONCA 112, 380 D.L.R. (4th) 506, 124 O.R. (3d) 481 (Ont. C.A.), leave to appeal refused *Peterborough Regional Health Centre v. Hesse*, 2015 CarswellOnt 16503, 2015 CarswellOnt 16504, [2015] S.C.C.A. No. 157 (S.C.C.): 280 patient records were accessed and the contact information was disclosed to unknown third parties without the consent of the patients. The Health Centre argued *PHIPA* exclusively occupied the field for civil breach of privacy claims and that the intrusion on seclusion claim was precluded by *PHIPA*. Justice Edwards, however, held that it was not plain and obvious that the inclusion on seclusion was precluded by the statute. The Health Centre appealed, and in another decision written by Justice Sharpe (Justices van Rensburg and Pardu concurring), the Court of Appeal upheld Justice Edward's decision.
10. On the issue on multijurisdictional class actions in Canada, see *Campbell v. Capital One Financial Corporation*, 2022 BCSC 928, 2022 CarswellBC 1463 (B.C. S.C.).
11. *Jones v. Tsige*, 2012 ONCA 32, 346 D.L.R. (4th) 34, 96 B.L.R. (4th) 1 (Ont. C.A.).
12. *Ibid*, at paras. 2, 4.

Justice Sharpe, for the Court, defined the tort of intrusion upon seclusion as being established when one intentionally intrudes, physically or otherwise, upon the seclusion of another or his private affairs or concerns, and the invasion would be highly offensive to a reasonable person.[13] It is a three-part test:

1. The intentional intrusion must be intentional or reckless, and without lawful justification.[14]
2. The information intruded upon must be private. For example, intrusions into financial or banking records,[15] health records,[16] sexual practices and orientation, employment, diary, or private correspondence.[17]
3. The intrusion must be "highly offensive", and could include distress, humiliation, or anguish.[18]

Cases following Jones have elaborated upon why the disclosure of some types of information is not offensive. For example, in *Broutzas v. Rouge Valley Health System*, the Court stated:[19]

> Generally speaking, 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. Contact information is publicly available and is routinely and readily disclosed to strangers to confirm one's identification, age, or address. People readily disclose their address and phone number to bank and store clerks, when booking train or plane tickets or when ordering a taxi or food delivery. Many people use their health cards for identification purposes. Save during the first trimester, the state of pregnancy, and the birth of

13. *Ibid*, at para. 71.
14. *Ibid*, at para. 72.
15. *Broutzas*, *supra*, footnote 4, at para. 165.
16. *Ibid*, at para. 165, citing *Daniells v. McLellan*, 2016 ONSC 3854, 267 A.C.W.S. (3d) 537, 2016 CarswellOnt 9865 (Ont. S.C.J.); *Hynes v. Western Regional Integrated Health Authority*, 2014 NLTD(G) 137, 64 C.P.C. (7th) 150, 1109 A.P.R. 138 (N.L. T.D.), and *Hemeon v. South West Nova District Health Authority*, 2015 NSSC 287, 24 C.C.L.T. (4th) 318, 80 C.P.C. (7th) 174 (N.S. S.C.).
17. *Jones, supra*, footnote 11, at para. 72; *Broutzas*, *supra*, footnote 4, at para. , citing *Drew v. Walmart Canada Inc.*, 2016 ONSC 8067, 276 A.C.W.S. (3d) 538, 2016 CarswellOnt 21013 (Ont. S.C.J.); *M.M. v. Lanark, Leeds and Grenville Children's Aid Society*, 2017 ONSC 7665, 287 A.C.W.S. (3d) 23, 2017 CarswellOnt 20451 (Ont. S.C.J.); and *Doucet v. The Royal Winnipeg Ballet*, 2018 ONSC 4008, 297 A.C.W.S. (3d) 250, 2018 CarswellOnt 10757 (Ont. S.C.J.), where the intrusion on seclusion were serious invasions of the class members' private matters and involved more than just contact information.
18. *Jones, supra*, footnote 11, at para. 71.
19. *Broutzas*, *supra*, footnote 4, at para. 153.

> child is rarely a purely private matter. The news of an anticipated birth and of a birth is typically shared and celebrated with family, friends, and colleagues and is often publicized.

Contact information is thus unlikely to be sufficient for a breach of privacy claim, whether grounded in intrusion upon seclusion or otherwise.

What about credit information? In *Broutzas*, Justice Perell reviewed Justice Leach's decision in *Powell v. Shirley*.[20] While negotiating an agreement of purchase and sale, the lawyers for the defendant vendors had obtained a credit report of the plaintiff purchasers, the Powells. They claimed a harmful intrusion upon their seclusion. Justice Leach dismissed their claim. The credit information was not private. Justice Perell explained Justice Leach's reasoning:[21]

> ...although the information contained in a credit report was financial information, it was not information in respect of which the Powells had a privacy interest. Information in credit reports about whether the Powells were judgment debtors was a matter of public record and non-private and there was no reasonable expectation of privacy. Further, Justice Leach held that a reasonable person knowing all the circumstances would not regard the obtaining of a credit report as highly offensive. Moreover, the lawyers had done nothing with the credit report other than put it their file, and, thus, Justice Leach concluded that any invasion of the Powell's privacy interest was not significant. Justice Leach also held the lawyers had a lawful justification for obtaining a credit report to which the Powells' privacy interest, if any, must yield.

More recently, in *Setoguchi v. Uber B.V.*,[22] Uber was alleged to have accessed information that included names, email addresses, telephone numbers, encrypted passwords, user IDs, user ratings, geolocation information, and in the case of drivers, driver's licence information, driver ratings and payment statements.[23] Uber argued

---

20. 2016 ONSC 3577, 267 A.C.W.S. (3d) 732, 2016 CarswellOnt 8853 (Ont. S.C.J.), additional reasons 2016 ONSC 5147, 270 A.C.W.S. (3d) 31, 2016 CarswellOnt 13016 (Ont. S.C.J.).
21. *Broutzas*, *supra*, footnote 4, at para. 156. See also *Larizza v. The Royal Bank of Canada*, 2017 ONSC 6140, 284 A.C.W.S. (3d) 516, 2017 CarswellOnt 15900 (Ont. S.C.J.) at para. 59, affirmed *Larizza v. Royal Bank of Canada*, 2018 ONCA 632, 296 A.C.W.S. (3d) 70, 2018 CarswellOnt 11406 (Ont. C.A.): "...credit checks do not give rise to [a legitimate privacy interest] because they tend to contain information about dealings with third parties". An appeal from the decision was dismissed: 2018 ONCA 632, 296 A.C.W.S. (3d) 70, 2018 CarswellOnt 11406 (Ont. C.A.).
22. 2021 ABQB 18, 72 C.C.L.T. (4th) 107, 63 C.P.C. (8th) 306 (Alta. Q.B.).
23. *Ibid*, at para. 6.

that this was not fairly described as private information, nor did it reveal intimate details of the individual. The Court agreed. It found that no one would have had, or did have, a reasonable expectation of privacy in the information.[24]

Thus, when considering a cybersecurity breach claim based on intrusion upon seclusion, the proposed plaintiff must consider whether the *Jones* criteria have been met, particularly regarding the sort of information accessed by the cyberhackers.

Equally as important as the kind of information impacted or accessed is the nature of the privacy intrusion itself. If a data breach has minimal impact on the affected parties, it is not appropriate to allow the claim of intrusion upon seclusion to proceed, even if the information is objectively sensitive.

In *Stewart v. Demme*, the defendant nurse committed a large narcotics theft over the course of ten years. In order to obtain access to the pills, the nurse viewed limited patient information of thousands of patients, some of whom were in her unit and some of whom were not. When the hospital finally discovered the thefts, it contacted all affected patients.

The patients brought a class proceeding seeking damages for intrusion upon seclusion and negligence. For reasons discussed later, Morgan J. certified the action as a class proceeding for intrusion upon seclusion and not negligence. The defendant nurse and hospital appealed the decision.

The Divisional Court (Sachs J., for the Court) overturned the certification judge's decision. Sachs J. wrote:[25]

> ...intrusion upon seclusion is a limited and specific tort developed for cases where there was a "deliberate and significant invasion" of "highly personal information" that would be "highly offensive to a reasonable person." While the information accessed was health information, the information accessed was limited and the access was fleeting and incidental to the medication theft.

Given the Divisional Court's reminder that only exceptional intrusions on informational privacy are actionable, those seeking to bring intrusion upon seclusion actions against cyber threat actors for breaches of privacy or other cybersecurity breaches, must ensure the intrusion was deliberate, significant, and highly offensive.

---

24. *Ibid*, at para. 52.
25. *Stewart v. Demme*, 2022 ONSC 1790, 81 C.C.L.T. (4th) 64, 161 O.R. (3d) 21 (Ont. Div. Ct.) at para. 3, additional reasons 2022 ONSC 2329, 2022 A.C.W.S. 1028, 2022 CarswellOnt 4934 (Ont. Div. Ct.), reversing 2020 ONSC 83, 63 C.C.L.T. (4th) 93, 315 A.C.W.S. (3d) 22 (Ont. S.C.J.).

B. Not So Obvious: No Intrusion By a "Database Defendant"

It took no time for intrusion upon seclusion, once consecrated as a nominate tort, to become the cause of action of choice for victims of cybersecurity attacks.

However, a theoretical question quickly emerged about "database defendants", parties with electronic databases of private information that are hacked by an unauthorized intruder. Could database defendants be liable for intrusion upon seclusion, where the third-party hacker is unknown?

For a brief period, the answer appeared to be "perhaps". Claims were allowed to proceed past a preliminary challenge. It was not plain and obvious that the tort could not include "database defendants" who recklessly enabled a hacker attack to occur.

Such was the case in *Agnew-Americano v. Equifax*. The facts in the proposed class action were not in dispute. The proposed representative plaintiff received a letter from Equifax on October 17, 2017. It confirmed that her personal information had been "compromised" and "impacted" by hackers. The letter said that the compromised information included her social insurance number, name, address, date of birth, phone number, email address, username, password, and secret question/answer.[26]

Equifax opposed certification, *inter alia*, for intrusion upon seclusion and for breach of provincial privacy legislation in failing to disclose a cause of action. Justice Glustein allowed the intrusion upon seclusion claim to proceed against Equifax.[27]

---

26. *Agnew-Americano v. Equifax Canada Co.*, 2019 ONSC 7110, 313 A.C.W.S. (3d) 694, 2019 CarswellOnt 20409 (Ont. S.C.J.) at para. 45, reversed *Owsianik v. Equifax Canada Co.*, 2021 ONSC 4112, 18 B.L.R. (6th) 78, 75 C.C.L.T. (4th) 243 (Ont. Div. Ct.), affirmed *Owsianik v. Equifax Canada Co.*, 2022 ONCA 813, 2022 A.C.W.S. 2838, 2022 CarswellOnt 16846 (Ont. C.A.).

27. *Ibid*, at paras. 103, 109, 110, 112, 113, 114, 118-129, 135; *Tucci v. Peoples Trust Company*, 2017 BCSC 1525, 283 A.C.W.S. (3d) 88, 2017 CarswellBC 2373 (B.C. S.C.) at para. 152, reversed in part 2020 BCCA 246, 451 D.L.R. (4th) 302, 69 C.C.L.T. (4th) 198 (B.C. C.A.); *Kaplan v. Casino Rama*, 2019 ONSC 2025, (*sub nom.* Kaplan v. Casino Rama Services Inc.) 145 O.R. (3d) 736, 305 A.C.W.S. (3d) 249 (Ont. S.C.J.) at paras. 28-29, additional reasons 2019 ONSC 3310, 306 A.C.W.S. (3d) 711, 2019 CarswellOnt 9260 (Ont. S.C.J.); *Bennett v. Lenovo (Canada) Inc.*, 2017 ONSC 1082, 276 A.C.W.S. (3d) 808, 2017 CarswellOnt 2314 (Ont. S.C.J.), at paras. 4, 18, 19, though the *Lenovo* case was somewhat different. The intrusion upon seclusion was alleged to have occurred because the defendant computer manufacturer pre-loaded laptops with a program that injected unauthorized advertisements which "allow[ed] hackers [...] to collect [...] bank credentials, passwords and other highly sensitive information". The claim for intrusion upon seclusion was not struck because Lenovo exposed its computer users to the risk of

That was then. The answer to the database defendant query now appears to be a more resounding "no".

The Ontario Divisional Court overturned Justice Glustein's decision and set aside the certification of the intrusion upon seclusion claim.[28] Justice Ramsay, for the Court, was clear that database defendants cannot be intruders within the scope of the tort, if they are not the ones who intruded:[29]

> The tort of intrusion upon seclusion was defined authoritatively only nine years ago. It has nothing to do with a database defendant. It need not even involve databases. It has to do with humiliation and emotional harm suffered by a personal intrusion into private affairs, for which there is no other remedy because the loss cannot be readily quantified in monetary terms. I agree that Sharpe J.A.'s definition of the tort is not necessarily the last word, but to extend liability to a person who does not intrude, but who fails to prevent the intrusion of another, in the face of Sharpe J.A.'s advertence to the danger of opening the floodgates, would, in my view, be more than an incremental change in the common law.
>
> I agree with my colleague [...] 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. [...]
>
> The plaintiffs here are not without remedy. The essence of their claim has to do with risk to economic interests caused by disclosure of their financial information. It is not too much to ask that they prove their damages. [...] The tort of negligence protects them adequately and has the advantage that it does not require them to prove recklessness.

Winder v. Marriott International, Inc. is another example of the tort's inability to capture database defendants, who are themselves victims of the intrusion.[30]

---

hacking, allegations similar to those in *Agnew-Americano*. A defendant who permits exposure to third parties by installing software or permitting software to be installed may not be different from a database defendant who allegedly recklessly allows hacking to take place, if it knows that its system is grossly deficient, and is advised of a high risk of exposure to its clients who store their personal financial information on the database, as alleged in *Agnew-Americano*.

28. *Owsianik v. Equifax Canada Co*., 2021 ONSC 4112, 18 B.L.R. (6th) 78, 75 C.C.L.T. (4th) 243 (Ont. Div. Ct.) at para. 58, affirmed 2022 ONCA 813, 2022 A.C.W.S. 2838, 2022 CarswellOnt 16846 (Ont. C.A.).
29. *Ibid*, at paras. 54-57.
30. *Winder v. Marriott International, Inc*., 2022 ONSC 390, 343 A.C.W.S. (3d)

The background to the case is not complex. Individuals provided personal information to make reservations at Marriott hotels. Marriott's reservations database was hacked. Importantly, Marriott was unaware of the hacker's activities for four years. When it finally discovered the breach, Marriott allegedly waited two months before taking remedial steps.[31] Marriott did not offer the affected individuals credit monitoring or other identity-protecting measures, nor did it offer compensation to the affected individuals.

Glenn Winder was granted carriage for a proposed national data breach class action against the Marriott Hotels chain. It was not disputed that the hacker would be liable for the tort of intrusion upon seclusion, as the hacker is the intruder. However, before the certification motion, the parties put forward a question of law, asking the Court to determine whether intrusion upon seclusion could viably be pleaded against Marriott.[32]

Marriott made the argument that it could not be liable for intrusion upon seclusion as it is not an intruder, but a victim of the intruder.[33]

Justice Perell declined Mr. Winder's submission to extend the law as argued in the *Equifax* cases. Instead. Justice Perell followed the developing, consistent line of cases stemming from Justice Ramsay's decision in the Equifax litigation. This led to the conclusion that it was not legally tenable to plead intrusion upon seclusion against Marriott.[34]

Mr. Winder had argued that by allowing the hacker into its database, Marriott was an intruder.[35] Perell J. disagreed, and supported his decision by citing at length from *Del Giudice v. Thompson*,[36] an earlier decision of his.

Del Giudice is helpful. It focused on the Capital One hack. The personal and confidential information of an estimated 6 million Canadian customers was misappropriated.[37] The identity of the alleged hacker was known. The plaintiffs commenced a class

124, 2022 CarswellOnt 641 (Ont. S.C.J.), affirmed 2022 ONCA 815, 2022 CarswellOnt 16872 (Ont. C.A.).

31. *Ibid*, at para. 3.
32. *Ibid*, at para. 2.
33. *Ibid*, at para. 4.
34. *Ibid*, at para. 7.
35. *Ibid*, at para. 9-10.
36. 2021 ONSC 5379, 71 E.T.R. (4th) 23, 337 A.C.W.S. (3d) 30 (Ont. S.C.J.). See *Campbell*, *supra*, footnote 10, at paras. 6, 103.
37. 2020 ONSC 2676, 320 A.C.W.S. (3d) 18, 2020 CarswellOnt 6043 (Ont. S.C.J.) at paras. 2-4, additional reasons 2020 ONSC 3623, 320 A.C.W.S. (3d) 23, 2020 CarswellOnt 8153 (Ont. S.C.J.).

proceeding. They sought certification of a number of claims, including intrusion upon seclusion against Capital One and the Amazon Web server holders.

Perell J. struck out the entire Statement of Claim without leave to deliver an amended pleading. Perell J. relied largely on Justice Ramsay's reasons in the Divisional Court's decision in *Owsianik*.[38] After quoting Justice Ramsay, Perell J. added:[39]

> Adding to what Justice Ramsey said, I would add that if the tort of intrusion on seclusion would assign liability without an intrusion, then it would assign liability to categories of misconduct that are adequately controlled by an assortment of other possible torts, by statutory provisions, and by actions for breach of contract. The Court of Appeal in *Jones v. Tsige*, however, intended intrusion on seclusion to fill gaps in the law of privacy not pave them over.

Perell J. rejected the idea that recklessness or negligence could satisfy the requirement of deliberate, wilful, purposeful, mindful conduct by the defendant for intrusion upon seclusion.[40]

Returning to the case before him in *Marriott*, Perell J. concluded that intrusion upon seclusion, as set out in *Jones v. Tsige*, was not intended to be a broad tort, and does not extend to constructive intruders.[41] It was Perell J.'s view that the tort did not need to be extended to fill a gap regarding wrongdoers in Marriott's position, because the law "associated with negligence, breach of confidence, breach of fiduciary duty, breach of contract, and breach of statute address [*sic*] or could address the pleaded circumstances of the immediate case."[42]

Perell J. concluded that the Statement of Claim did not disclose a cause of action against Marriott for intrusion upon seclusion.[43]

In June 2022, the Ontario Court of Appeal heard three grouped appeals, arising from the class actions in *Owsianik, Odobo*,[44] and *Winder*. Each of the plaintiffs appealed from the Court's refusal or determination not to certify their intrusion upon seclusion claims against the "Database Defendants".

38. *Del Giudice*, *supra*, footnote 36, at para. 8.
39. *Ibid*, at para. 138.
40. *Ibid*, at paras. 144-145; *Broutzas, supra*, footnote 4, at para. 211.
41. *Marriott*, *supra*, footnote 30, at para. 13.
42. *Ibid,* at para. 14.
43. *Ibid,* at para. 18.
44. See *Obodo v. Trans Union of Canada, Inc*., 2021 ONSC 7297, 2021 CarswellOnt 15509 (Ont. S.C.J.) at para. 22, leave to appeal refused 2022 ONSC 1184, 2022 A.C.W.S. 256, 2022 CarswellOnt 2622 (Ont. Div. Ct.), affirmed 2022 ONCA 814, 2022 CarswellOnt 16847 (Ont. C.A.). See also *Campbell*, *supra*, at paras. 96-104.

In November 2022, the Ontario Court of Appeal dismissed all three appeals.[45] Doherty J.A., writing for the Court, observed as follows (referring to all three appeals):[46]

> 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. [...] The identity of the hackers is unknown.
>
> 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. [...] 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.

Justice Doherty acknowledged the danger in imposing liability for the tort of intrusion upon seclusion on database defendants who do not actually intrude on information:[47]

> 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. [...]
>
> 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.

Given the Ontario Court of Appeal's definitive conclusions in this line of cases, and barring any turnaround in the Supreme Court of Canada, it would now appear that intrusion upon seclusion cannot

45. *Owsianik v. Equifax Canada Co*., 2022 ONCA 813, 2022 A.C.W.S. 2838, 2022 CarswellOnt 16846 (Ont. C.A.); *Obodo v. Trans Union of Canada, Inc*., 2022 ONCA 814, 2022 CarswellOnt 16847 (Ont. C.A.); *Winder v. Marriott International, Inc*., 2022 ONCA 815, 2022 CarswellOnt 16872 (Ont. C.A.).
46. *Owsianik, ibid*, at paras. 7-8.
47. *Owsianik, ibid*, at paras. 65-66.

extend to database defendants who are not themselves intruders. Negligence alone, as Justice Doherty notes, cannot morph or be transformed into an intentional tort.[48]

C. What Are Your Options? Negligence, Breach of Contract, Breach of Confidence, Fiduciary Duty

Negligence

The elements of negligence are well known:

(1) the defendant owes the plaintiff a duty of care;
(2) the defendant's behaviour breached the standard of care;
(3) the plaintiff suffered compensable loss;
(4) the damages were caused in fact by the defendant's breach; and,
(5) the damages are not too remote in law.[49]

Negligence claims are problematic in privacy and cybersecurity cases. The compensable loss element is usually lacking. Negligence liability is based on harm. Society and the common law have set a high, if not impossible, bar for compensable loss where a cybersecurity breach entails privacy violations.

In *Stewart v. Demme*, discussed above, Morgan J. held that a plaintiff whose private health information had been invaded was ineligible to ground a claim in negligence, where she suffered no actual damage beyond the fact of the invasion:[50]

> ...[while] invasion of privacy is itself a form of harm, [it]... is not the type of harm that suffices for a negligence claim. Unlike intrusion against seclusion, which is one of the few areas of tort law allowing for "symbolic" or "moral damages", negligence liability requires that actual harm be manifest and caused by the wrong.

As noted, Morgan J.'s decision was overturned on appeal. This does not alter the principle that actual damages or harm is necessary for a pleading in negligence to survive a challenge.

---

48. *Owsianik, ibid*, at para. 71.
49. *Del Giudice*, *supra*, footnote 36, at para. 222.
50. 2020 ONSC 83, 63 C.C.L.T. (4th) 93, 315 A.C.W.S. (3d) 22 (Ont. S.C.J.) at para. 86, additional reasons 2020 ONSC 1335, 63 C.C.L.T. (4th) 127, 316 A.C.W.S. (3d) 21 (Ont. S.C.J.), reversed 2022 ONSC 1790, 81 C.C.L.T. (4th) 64, 161 O.R. (3d) 21 (Ont. Div. Ct.), additional reasons 2022 ONSC 2329, 2022 A.C.W.S. 1028, 2022 CarswellOnt 4934 (Ont. Div. Ct.).

The plaintiffs in *Del Giudice*, discussed above, also framed their claim against Capital One and Amazon Web in negligence and breach of the duty to warn.[51] Perell J. found it to be plain and obvious that the plaintiffs and the class members did not have legally viable and certifiable causes of action on either ground.[52]

Regarding the negligence claim, Perell J. explained:

> [...] the overwhelming majority of the six million Canadians affected by the data breach will not have suffered harm compensable by the tort of negligence [...] because negligence law does not recognize as compensable harm upset, disgust, anxiety, agitation or mere psychological upset that does not cause a serious and prolonged injury and that does do not rise above the ordinary annoyances, anxieties and fears that people living in society routinely experience.[53]

Perell J. acknowledged that, for the minority who did suffer harm, the losses would be purely economic. Pure economic loss is economic loss unconnected to physical or mental injury to the plaintiff's person, or to physical damage to property.[54] Canadian tort law awards damages for pure economic loss only in rare circumstances.[55]

The requirements for a viable pure economic loss claim are beyond the scope of this paper.[56] Suffice to say, a cybersecurity breach victim bringing an action in negligence will need to have compensable harm or injury from the breach to be successful.

The Alberta Court of Queen's Bench engaged in a similar analysis in *Setoguchi*, discussed above. The proposed class proceeding arose from a 2016 hack by third parties or "unauthorized external actors" of Uber's store of drivers' and users' personal information or data.[57] Rooke J. dismissed the certification motion, persuaded by Uber's arguments that (1) there was no chance of loss, as the personal contact information was already in the public domain; (2) there was no evidence of harm or loss; and (3) conversely, there was evidence of no harm or loss.[58]

---

51. *Del Giudice*, *supra*, footnote 36, at para. 219.
52. *Ibid,* at para. 222.
53. *Ibid,* at paras. 223-224.
54. *Ibid,* at para. 230. In *Del Giudice*, the overwhelming majority of the Class Members will have suffered only the threat of pure economic losses. Only a few may have suffered actual pure economic loss from identify theft and fraud, or from expending money to respond to the threat of a fraud occurring.
55. *Ibid,* at para. 226.
56. *1688782 Ontario Inc. v. Maple Leaf Foods Inc.*, 2020 SCC 35, 450 D.L.R. (4th) 181, 69 C.C.L.T. (4th) 1 (S.C.C.) is the most recent Supreme Court review of this area of damages.
57. *Setoguchi*, *supra*, footnote 22, at para. 1.

More recently, the British Columbia Supreme Court certified a negligence class proceeding arising from a cyberattack. In *Campbell v. Capital One Financial Corporation*,[59] Paige Thompson hacked Capital One's database and downloaded the personal and financial information of American and Canadian residents who had applied for Capital One credit cards between 2005 and early 2019. (The *Del Giudice* action arises from the same set of facts, but in Ontario.).

In *Campbell*, Capital One argued that the proposed representative plaintiff had not adequately pleaded (i) the existence of a duty of care, (ii) that he suffered compensable damages, or (iii) causation.[60] The duty of care was defined as a duty to keep personal information confidential and secure, and to ensure it would not be lost, disseminated, or disclosed to unauthorized persons.[61] Campbell pleaded damages for emotional distress, increased risk of harm, and the costs of mitigating against that risk.

Iyer J. agreed that the first two categories require actual losses, but expenses actually incurred to mitigate against the risk of future loss are compensable damages and satisfy the third element of a negligence claim.[62] For these reasons, Iyer J. agreed the pleadings disclosed a cause of action in negligence.[63]

In sum, negligence requires proof of damage, and the victim of a cybersecurity breach may not have the requisite proof of damage, under current Canadian tort law principles.

Breach of Contract

The law on breach of contract imposes its own limitations regarding cybersecurity breaches.

Primarily, and obviously, the cyberattack victim plaintiff needs to be party to a validly formed contract with the defendant, and that defendant needs to have breached their obligations under the contract.[64]

A number of cases have recognized privacy policies or other terms of use as the contract between the parties, for the purposes of a

58. *Ibid*, at para. 10.
59. 2022 BCSC 928, 2022 CarswellBC 1463 (B.C. S.C.), at paras. 1-4. See also *Botterell v. Capital One Bank (Canada Branch)*, 2021 BCCA 348, 80 C.P.C. (8th) 82, 336 A.C.W.S. (3d) 30 (B.C. C.A.).
60. *Campbell, ibid,* at para. 48.
61. *Ibid*, at para. 49.
62. *Ibid*, at paras. 53, 54.
63. *Ibid*, at para. 58.
64. *Del Giudice*, *supra*, footnote 36, at para. 252.

breach of contract claim.[65] However, the damages question is the challenge.

In the Equifax litigation, a subclass of class members had a contract with Equifax during the period of the breach, but their information was not accessed through the cyberattacks. The pleading for these parties focussed on Equifax's contractual obligations to protect personal information under its control.[66] Equifax argued that allowing a breach of contract claim for restitutionary or nominal damages to these plaintiffs would open the floodgates to litigation by those whose data was not actually intruded upon or otherwise accessed.[67]

Glustein J. rejected the argument, concluding that the breach of contract claim could proceed as it disclosed a cause of action for restitutionary and nominal damages.[68] In the Divisional Court, Equifax did not appeal that ruling.[69]

Some claimants have attempted to frame actions against database defendants or cyberattackers as breaches of the duty of good faith in the performance of a contract.

Evans v. Bank of Nova Scotia was one such case.[70] Customers of the Bank of Nova Scotia brought a proposed class proceeding against the Bank and a rogue bank employee, Richard Wilson, for damages, alleging several causes of action.

Mr. Wilson, the "intruder", had admitted to providing private and confidential information of approximately 643 Bank customers to his girlfriend, who then disseminated the private information to

65. *Evans v. Bank of Nova Scotia*, 2014 ONSC 2135, 55 C.P.C. (7th) 141, 241 A.C.W.S. (3d) 32 (Ont. S.C.J.), leave to appeal refused 2014 ONSC 7249, 247 A.C.W.S. (3d) 764, 2014 CarswellOnt 17769 (Ont. S.C.J.); *Hynes v. Western Regional Integrated Health Authority*, 2014 NLTD(G) 137, 64 C.P.C. (7th) 150, 1109 A.P.R. 138 (N.L. T.D.); *Daniells v. McLellan*, 2017 ONSC 3466, 39 C.C.L.T. (4th) 263, 6 C.P.C. (8th) 317 (Ont. S.C.J.), additional reasons 2017 ONSC 6887, 47 C.C.L.T. (4th) 337, 14 C.P.C. (8th) 303 (Ont. S.C.J.); *Kaplan v. Casino Rama*, 2019 ONSC 2025, (*sub nom.* Kaplan v. Casino Rama Services Inc.) 145 O.R. (3d) 736, 305 A.C.W.S. (3d) 249 (Ont. S.C.J.), additional reasons 2019 ONSC 3310, 306 A.C.W.S. (3d) 711, 2019 CarswellOnt 9260 (Ont. S.C.J.); *Tocco v. Bell Mobility Inc.*, 2019 ONSC 2916, 305 A.C.W.S. (3d) 705, 2019 CarswellOnt 7321 (Ont. S.C.J.), additional reasons 2019 ONSC 4021, 307 A.C.W.S. (3d) 263, 2019 CarswellOnt 10550 (Ont. S.C.J.).
66. *Agnew-Americano, supra*, footnote 26, at para. 243*ff.*
67. *Ibid,* at para. 262.
68. *Ibid,* at para. 301.
69. *Owsianik, supra*, footnote 38, at para. 4.
70. 2014 ONSC 2135, 55 C.P.C. (7th) 141, 241 A.C.W.S. (3d) 32 (Ont. S.C.J.), leave to appeal refused 2014 ONSC 7249, 247 A.C.W.S. (3d) 764, 2014 CarswellOnt 17769 (Ont. S.C.J.), at para. 37.

third parties for fraudulent and improper purposes. As a result, approximately 138 of the Bank's customers became victims of identity theft and fraud, which negatively affected their credit rating.[71] The Bank compensated these victims for their monetary losses and offered all affected individuals a complimentary subscription to a credit monitoring and identity theft protection service.[72]

Among the causes of action that the plaintiff alleged was breach of the duty of good faith by both Mr. Wilson and the Bank.

Smith J. readily concluded that there was no free-standing duty of good faith, but that Mr. Wilson had acted in bad faith, and in his own self-interest, by providing the personal and confidential information for an improper purpose.[73] Against the Bank, Smith J. found that the plaintiff had not alleged it to have acted in bad faith, but even if there was a duty of good faith, the Bank had not breached it.[74]

Breach of Confidence

Breach of confidence is not commonly pleaded in cybersecurity or privacy actions. A party seeking to recover for breach of confidence must establish that the information was confidential in nature, that it was disclosed in circumstances creating an obligation of confidentiality, and that its unauthorized use was detrimental to the plaintiff.[75]

However, breach of confidence in cybersecurity cases appears to suffer from the same problem as the intrusion upon seclusion tort. In most instances, the victim has given their private data to a database defendant, and not to the party who ultimately discloses it, the cyberattacker, or the recipient of the cyberattacker's stolen data.

In *Kaplan*, the Court zeroed in on this problem. It concluded that the defendants' failure to prevent a cyberattack was not a 'misuse' of confidential information, within the meaning of the tort.[76]

Breach of Fiduciary Duty

Like breach of confidence, breach of fiduciary duty is not often pleaded.

71. *Ibid*, at paras. 2-5.
72. *Ibid*, at paras. 2-5.
73. *Ibid*, at paras. 45, 46.
74. *Ibid*, at para. 45.
75. *Lac Minerals Ltd. v. International Corona Resources Ltd.*, [1989] 2 S.C.R. 574, 61 D.L.R. (4th) 14, 26 C.P.R. (3d) 97 (S.C.C.).
76. *Kaplan, supra*, footnote 27, at para. 30.

In *Evans*, one of the issues before Smith J. was whether the Bank was liable for a breach of fiduciary duty (as well as a duty of good faith, discussed above). The plaintiff pleaded that the Bank owed the class a fiduciary duty based on the business relationship between them. Since the class trusted the Bank with possession of their information, it had a reasonable expectation that the information would be kept safe and secure, and used only for proper business purposes. The plaintiff alleged that the bank had profited from the business relationship when it divulged the confidential, personal, and financial information to third parties.[77]

Smith J. reviewed the law of fiduciary duties.[78] In particular, the Court looked at the settled law confirming that, absent a special relationship or exceptional circumstances, the relationship between a bank and customers is that of a debtor and creditor.[79]

Smith J. found there was no basis in fact that a special relationship or exceptional circumstances existed that justified imposing a fiduciary duty on the Bank with regards to its customers.[80] That said, a fiduciary duty claim may be more appropriate in the context of a privacy or cybersecurity breach where the underlying relationship is one the law recognizes as fiduciary, like the physician-patient relationship.[81]

D. The Door Is Not Closed: Other Important Privacy Torts

Some privacy torts may find themselves more frequently invoked as technology advances.

Public Disclosure of Private Facts

The tort of public disclosure of private facts was first recognized in Canada in *Jane Doe 464533 v. D.(N.)*.[82]

The tort is established when one gives publicity to the private life of another by publicly disclosing a matter that is not of legitimate concern to the public, and the disclosure would be highly offensive to a reasonable person.[83]

77. *Evans, supra*, footnote 65, at para. 39.
78. *Evans, ibid,* at para. 41, citing *Frame v. Smith*, [1987] 2 S.C.R. 99, 42 D.L.R. (4th) 81, 42 C.C.L.T. 1 (S.C.C.), at para. 60.
79. *Evans, ibid,* at paras. 42-43.
80. *Ibid,* at para. 44.
81. *McInerney v. MacDonald*, [1992] 2 S.C.R. 138, 93 D.L.R. (4th) 415, 12 C.C.L.T. (2d) 225 (S.C.C.).
82. 2016 ONSC 541 2016 ONSC 541, 394 D.L.R. (4th) 169, 25 C.C.L.T. (4th) 19 (Ont. S.C.J.) (*Jane Doe #1*).
83. *Ibid*, at para. 46.

In *Jane Doe 464533 v. D. (N.)*, the plaintiff's ex-boyfriend had posted an intimate video of her on a pornography website without her knowledge or consent. The video was viewed by her acquaintances.[84] The plaintiff brought an action for compensatory damages, punitive damages, and injunctive relief.[85] The action was heard as a default proceeding.[86] Although the default judgment was later set aside,[87] the decision stands as the starting point for the tort of public disclosure of private facts.

Justice Stinson reviewed the Court of Appeal for Ontario's recognition of intrusion upon seclusion in *Jones v. Tsige* as one of four possible invasion of privacy torts identified in American legal commentary.[88] His Honour concluded that the plaintiff's case fell within the tort of "public disclosure of private facts",[89] and that Ontario law required the recognition of such a remedy.[90] Justice Stinson introduced into Ontario law the elements of the tort described above.

When the default judgment was set aside, so too was the novel and necessary advancement in the law that was the tort of public disclosure of private facts. However, Justice Gomery revived it in *Jane Doe 72511 v. N.M. et al.*[91]

The plaintiff's boyfriend in that case had likewise posted sexually explicit content of the plaintiff on a pornographic website without her knowledge or consent. He was convicted of criminal assault and battery against her.[92]

The plaintiff sued the defendant for assault, battery, and for posting the video without her consent, and his parents for negligence.[93] The matter was also heard as a default proceeding.[94]

The judgment in Jane Doe #1 having been set aside, Justice Gomery started with the proposition that no civil right of action existed in Ontario for the posting of intimate images without consent

84. *Ibid,* at para. 8.
85. *Ibid*, at para. 1.
86. *Ibid*, at para. 3.
87. *Jane Doe 464533 v. D. (N.)*, 2016 ONSC 4920, 276 A.C.W.S. (3d) 55, 2016 CarswellOnt 21212 (Ont. S.C.J.), leave to appeal refused 2017 ONSC 127, 276 A.C.W.S. (3d) 261, 2017 CarswellOnt 163 (Ont. S.C.J.).
88. *Ibid*, at paras. 34-36.
89. *Ibid*, at para. 41.
90. *Ibid*, at para. 45.
91. 2018 ONSC 6607, 53 C.C.L.T. (4th) 289, 143 O.R. (3d) 277 (Ont. S.C.J.) (*Jane Doe #2*).
92. *Ibid*, at paras. 1, 8.
93. *Ibid*, at para. 32.
94. *Ibid*, at para. 8.

and considered whether the tort of public disclosure of private facts should be recognized in the province.[95]

His Honour concluded, as Justice Stinson had, that the best way to fashion a civil remedy for this kind of misconduct was to adopt the tort of public disclosure of private facts in Ontario. To do so would be consistent with Charter of Rights and Freedoms values, and would be a constructive, incremental modification of existing law to address a challenge posed by new technology.[96]

Relying on Justice Stinson's framework, Justice Gomery ruled that the plaintiff must establish that (1) the defendant had publicized an aspect of the plaintiff's private life; (2) the plaintiff did not consent to the publication; (3) the matter publicized or its publication would be highly offensive to a reasonable person; and (4) the publication was not of legitimate concern to the public.[97]

Justice Gomery found the elements to be satisfied in the case before him. By posting the explicit video, the defendant had publicly disclosed an aspect of the plaintiff's private life, to which the plaintiff had not consented. A reasonable person would consider the posting of the video highly offensive, since it showed Jane's face and body, and allowed strangers to see her engaged in sexual activity. Nothing about the video gave the public a legitimate interest in its publication.[98]

The Alberta and Nova Scotia courts have also recognized the tort of public disclosure of private facts.[99]

Public disclosure of private facts is not without its own limits. As with intrusion upon seclusion, there is no tort of public disclosure where the affected individual authorized the disclosure or publicity of their information.[100]

Also, like intrusion upon seclusion, the information or facts at issue must be "private". The question of what is "private" requires more room than this paper can offer. Simplifying, facts in the public domain are not private.[101] Routinely private matters - sexual relations, family issues, health issues - are.[102]

---

95. *Ibid*, at paras. 60-61.
96. *Ibid*, at paras. 86-87, 93.
97. *Ibid*, at para. 99.
98. *Ibid*, at para. 100.
99. *Racki v. Racki*, 2021 NSSC 46, 72 C.C.L.T. (4th) 310, 52 R.F.L. (8th) 1 (N.S. S.C.); *ES v. Shillington*, 2021 ABQB 739, 78 C.C.L.T. (4th) 253, [2021] 12 W.W.R. 540 (Alta. Q.B.); *LDS v. SCA*, 2021 ABQB 818, 341 A.C.W.S. (3d) 108, 2021 CarswellAlta 2576 (Alta. Q.B.).
100. Sarit K. Mizrahi, "Ontario's New Invasion of Privacy Torts: Do They Offer Monetary Redress for Violations Suffered via the Internet of Things?", (2018) 8:1 online: UWO J Leg Stud 3, n. 113, 114.

Beyond these decisions lies a large, theoretical debate. Some scholars view the refusal to recognize a degree of privacy within public spheres as nonsensical, especially in the digital age.[103] The Supreme Court of Canada has recognized, in at least one limited instance, that privacy can be invaded in the public sphere.[104] However, the issue remains an open one.

Appropriation of Personality

The tort of appropriation of personality protects the right of a person to control the use of their name and likeness for commercial purposes. It is actionable where the defendant has appropriated for their own purposes some attribute of the plaintiff's name or identity.[105]

This tort has not appeared often in the context of cyberattacks or cybersecurity breaches. However, in Del Giudice, the plaintiffs introduced an interesting perspective on the tort when they claimed that Capital One and Amazon Web were liable for the intentional and/or reckless misappropriation of their financial personality.[106]

The plaintiffs argued that "personality" includes a person's "unique financial personality which is a reflection of his or her character, traits, values, and behaviours", and that Capital One traded on this personality by "collecting and merchandizing the personal information for its own financial gain" without authorization, causing damage.[107]

Perell J. hesitantly accepted that a person may have a unique financial personality. His Honour found, however, that the plaintiffs' claim could not fit within the existing tort of misappropriation of personality. Extending the tort to cover the plaintiffs' claims would go beyond an incremental, appropriate development in the law.[108]

Perell J. stated:[109]

> The gravamen of the existing tort is the usurpation of the plaintiff's right to control and market his or her personality. More precisely, the gravamen of the tort is the usurpation of the plaintiff's right to be paid for

101. *Supra*, footnote 87.
102. *Ibid.*
103. *Supra*, footnote 97.
104. *Supra*, footnote 108.
105. Lewis N. Klar, *Remedies in Tort*, s. 27.4.
106. *Del Giudice, supra*, footnote 37, at para. 148.
107. *Ibid*, at para. 149.
108. *Ibid*, at paras. 150-152.
109. *Ibid*, at paras. 151-152.

> testimonials and product endorsements. There has to be damage to a person's right to exploit his or her personality for commercial purposes. [...]
>
> I will grant the Plaintiffs the notion that a person may have a unique financial personality. The celebrities who went from rags to riches or from riches to rags would be examples, but it is plain and obvious that the tort of misappropriation of personality is not available in the circumstances of the immediate case. In the immediate case there is nothing of an endorsement or testimonial in the Class Members' application for credit cards and filling out application forms [...], there is no misappropriation and the Class Members consented to the gathering and the use of their financial information [...], there is no use of the personal information to endorse Capital One's products or services [...], there is no damage to the Class Members' right to exploit their personality for commercial purposes.

Vicarious Liability

What is the situation where an individual entrusts a corporation with their private and confidential information, and a rogue employee intrudes or discloses that information without the victim's, or the corporation's, consent?

In *Evans*, discussed above, Smith J. considered whether the Bank of Nova Scotia could be vicariously liable for intrusion upon seclusion by Mr. Wilson, given that he had acted without the Bank's knowledge or authorization.[110] The Bank argued that it could not be vicariously liable for Mr. Wilson's deliberate conduct.[111]

Smith J. found that even though the Bank was not involved in Mr. Wilson's improper conduct, it arguably created the opportunity for Mr. Wilson to steal the customer information by allowing him unsupervised access to the client files.

Smith J. reviewed the law on employers' vicarious liability for their employees' misconduct. It provides that employers may justly be held liable where the act falls within the ambit of the risk that the employer's enterprise creates or exacerbates, and the act is sufficiently related to conduct authorized by the employer to justify the imposition of vicarious liability.[112]

---

110. *Evans, supra*, footnote 65, at paras. 6, 19.

111. *Ibid.*

112. *Ibid*, at paras. 20-21, 26, 94, citing *Bazley v. Curry*, [1999] 2 S.C.R. 534, 174 D.L.R. (4th) 45, 43 C.C.E.L. (2d) 1 (S.C.C.), at paras. 37, 41; *Blackwater v. Plint*, 2005 SCC 58, [2005] 3 S.C.R. 3, 258 D.L.R. (4th) 275 (S.C.C.), at para. 20.

Smith J. concluded that it was not plain and obvious that the claim against the Bank in vicarious liability would not succeed, and certified it as a common issue in the class proceeding:[113]

> In this case, the Bank created the opportunity for Wilson to abuse his power by allowing him to have unsupervised access to customers' private information without installing any monitoring system. [...] Wilson was given complete power in relation to the victims' (customers) confidential information, because of his unsupervised access to their confidential information.
>
> Bank customers are entirely vulnerable to an employee releasing their confidential information. Finally, there is a significant connection between the risk created by the employer in this situation and the wrongful conduct of the employee. [...] While the Bank itself was not directly involved in the improper access of customer information, vicarious liability "is strict, and does not require any misconduct on the part of the person who is subject to it. [citations omitted][114]

E. Other Considerations

Class Action As a Vehicle for Litigation

Cybersecurity breaches tend to affect multiple individuals at once. For that reason, class proceedings have become a vehicle of choice for large-scale cybersecurity breaches, as the reader may have inferred from repeated mentions of above.

For example, the 2017 intrusion into Equifax's data gave rise to six class proceedings in Canada, as almost 20,000 Canadians were affected.[115]

More recently, in *Sweet v. Canada*, the Federal Court certified a class action which saw hackers breach Government of Canada websites, and gain access to the personal, financial and other information of thousands of Canadians.[116]

However, while these class actions cases are of some assistance in understanding the options available to an affected individual, they

113. *Evans, supra*, footnote 65, at paras. 22-23, 95.

114. For an expansive summary of vicarious liability in breach of privacy actions, see Barbara von Tigerstrom, Direct and Vicarious Liability for Tort Claims Involving Violation of Privacy, 2018 96-3 Canadian Bar Review 539, 2018 CanLIIDocs 295.

115. *Johnson v. Equifax Inc.*, 2018 SKQB 305, 299 A.C.W.S. (3d) 262, 2018 CarswellSask 546 (Sask. Q.B.), at para. 2.

116. *Sweet v. Canada*, 2022 FC 1228, 86 C.C.L.T. (4th) 79, 2022 CarswellNat 3382 (F.C.), at para. 1.

are of limited precedential value. As Justice Perell, an experienced class proceedings judge, observed in *Karasik*, "privacy breach class actions [...] are a burgeoning genre of cases but nascent because, although many cases have been certified, none have yet proceeded to a trial."[117] For these reasons, privacy breach class actions are in a state of flux.[118]

Class proceedings can be appropriate where individuals have been affected in different ways, as they allow for flexibility. For example, in *Agnew-Americano*, the proposed class included two subclasses, based on whether the affected individuals also purchased subscription products from Equifax during the period of the breach.

Class proceedings case also help to demonstrate the kinds of settlements available to affected individuals. *Karasik v. Yahoo Inc.* involved multiple cyberattacks by the Federal Secret Service of the Russian Federation in 2013, 2014, and 2016 on Yahoo Inc. and Yahoo! Canada Co. They resulted in the exposure of 5 million Canadians' personal information.[119]

These attacks gave rise to a class action in 2016, advancing various privacy torts (including intrusion upon seclusion), negligence, and other restitutionary and statutory claims arising from the data breach.[120]

The parties to the class proceeding in *Karasik* reached a settlement that came before Justice Perell for approval.[121] Justice Perell offers a useful and authoritative summary review of the major or main causes of action advanced in reported privacy class actions.[122] The decision is also useful guide on quantum, based on its summary of 11 recent privacy case settlements.[123]

Needless to say, not every class proceeding is certified or allowed to proceed. Some notable class proceedings arising out of serious cybersecurity breaches have failed to overcome the certification bar. In *Simpson v. Facebook*[124] and *Kish v. Facebook Canada Ltd.*,[125] the

117. 2021 ONSC 1063, at para. 125 (*Karasik 2*).
118. *Redublo v. CarePartners*, 2022 ONSC 1398, 2022 CarswellOnt 2623 (Ont. S.C.J.), at para. 60.
119. *Karasik v. Yahoo Inc.*, 2019 ONSC 4670, 308 A.C.W.S. (3d) 481, 2019 CarswellOnt 12868 (Ont. S.C.J.) at paras. 1-2, additional reasons 2019 ONSC 5514, 310 A.C.W.S. (3d) 257, 2019 CarswellOnt 15233 (Ont. S.C.J.).
120. *Karasik 2*, at para. 42.
121. *Ibid*, at para. 431.
122. *Ibid*, at para. 13.
123. *Ibid*, at para. 136.
124. 2021 ONSC 968, 329 A.C.W.S. (3d) 695, 2021 CarswellOnt 1822 (Ont. S.C.J.), affirmed *Simpson v. Facebook, Inc.*, 2022 ONSC 1284, 469 D.L.R. (4th) 699, 160 O.R. (3d) 629 (Ont. Div. Ct.), at para. 2.

Ontario and Saskatchewan courts refused to certify the respective proposed class proceedings arising from the Cambridge Analytica data breach. There was no evidence that Canadian Facebook users had suffered an inappropriate breach of privacy or disclosure or private information.

What Kinds of Damages Are Available?[126]

Another consideration is damages.

As the Court of Appeal for Ontario has stated, mathematical exactitude in the calculation of damages is neither necessary nor realistic in many cases.[127] Judges must do their best to assess the damages suffered by a plaintiff on the available evidence, even where difficulties in their quantification make a precise calculation uncertain or impossible. This applies to privacy and cybersecurity breaches at common law.

Before *damages*, there must be *damage*.[128] In *Setoguchi*, the Alberta Court of Queen's Bench declined to certify a class proceeding arising out of a data breach because there was no evidence that any individuals had suffered harm or loss, and conversely, there was evidence that no individuals had suffered harm or loss.[129] The Court was critical of actions lacking such evidence:[130]

> There must be some evidence or basis in fact in support of real (not *de minimis*) compensable harm or loss, leading to a claim that is at least arguable, and that certification should indeed must not be allowed without it. Otherwise, a class proceeding could be a mere "fishing trip" based on speculation, without any evidence of fish being present.

The same challenge was identified by the Court in *Redublo v. CarePartners*: Where neither representative plaintiff nor any known class member has suffered pecuniary damages as a result of the hack,

125. 2021 SKQB 198, 335 A.C.W.S. (3d) 324, 2021 CarswellSask 478 (Sask. Q.B.), at paras. 6, 7 and 90.
126. For a review of damages for intrusion upon seclusion and public disclosure of private facts, see Mizrahi, *supra*.
127. *TMS Lighting Ltd. v. KJS Transport Inc.*, 2014 ONCA 1, 80 C.E.L.R. (3d) 167, 40 R.P.R. (5th) 171 (Ont. C.A.), at para. 61.
128. "Damage is the loss needed to make out the cause of action. [It] is the condition of being worse off than before entering into the transaction. Damages, on the other hand, is the monetary measure of the extent of that loss": *Hamilton (City) v. Metcalfe & Mansfield Capital Corp.*, 2012 ONCA 156, 347 D.L.R. (4th) 657, 290 O.A.C. 42 (Ont. C.A.), at para. 54.
129. *Setoguchi*, *supra*, footnote 22, at paras. 28-30.
130. *Ibid*, at paras. 37, 45.

the action was vulnerable to an argument that the class suffered no quantifiable harm.[131]

One factor that may affect damage is evidence that parties have experienced fraud or identity theft as a result of the cyberattack.[132] In *Kaplan*, Belobaba J. refused to certify an action where a hacker stole the personal information of the defendant's employees, customers, and suppliers. The personal information included varying combinations of name, address, date or birth, SIN, bank account details, and photographs.

In deciding to refuse the class action, Belobaba J. gave weight to the absence of evidence that any affected individuals had experienced fraud or identity theft, and that the bank had replaced all the money that was stolen.[133]

Even where there is damage – *i.e.*, loss or harm – fixing an appropriate quantum of compensatory damages is challenging. As noted, most of the available decision on quantum involving cybersecurity breaches come from court-approved settlements in class proceedings.

In *Mallette v. Bank of Montreal*,[134] Smith J. approved a settlement for $21,223,975 for a data breach at the Bank of Montreal that affected 113,151 clients, and $1,769,425 for a data breach that affected 10,101 Canadian Imperial Bank of Commerce clients. Both cases were ransomware attacks. Hackers breached the banks' IT systems and demanded ransom payments, failing which they threatened to publish client information on the Internet.[135] About 100 people did have their information published online.[136]

In both settlements, larger amounts were proposed for persons who had their social insurance number and date of birth information compromised, as opposed to class members who did not. Smith J. agreed the distinction was warranted since social insurance information is particularly sensitive and can be used to obtain more personal information to invade privacy.[137] Both banks also

131. *Redublo v. CarePartners*, 2022 ONSC 1398, 2022 CarswellOnt 2623 (Ont. S.C.J.), at para. 61.
132. *Kaplan, supra*, footnote 27, at para. 21.
133. *Ibid*, at para. 79.
134. 2021 ONSC 2924, 333 A.C.W.S. (3d) 254, 2021 CarswellOnt 5633 (Ont. S.C.J.), at paras. 1-2 [*Mallette*]. See also *Bannister v. Canadian Imperial Bank of Commerce*, 2021 ONSC 2927, 333 A.C.W.S. (3d) 253, 2021 CarswellOnt 5635 (Ont. S.C.J.).
135. *Mallette, ibid*, at para. 3.
136. *Ibid*, at para. 6.
137. *Ibid*, at para. 36.

offered affected customers two years of complimentary credit monitoring.[138]

In *Karasik*, Justice Perell performed a quantitative review of various settlements in Canadian class actions involving privacy and cybersecurity breaches. His Honour concluded:[139]

> The settlements in the above sample, by and large, reveal that Class Counsel's aspirations for enormous per capita awards of general damages (moral or symbolic damages) for intrusion on seclusion or breach of privacy statutes have been rebuffed by the settling defendants. It seems that it will take a trial decision awarding more than notional-nominal general damages, to break the will of defendants, who as I have already noted are sustained by the strength of their defences on causation and by the difficulties associated with proving negligence or the wilfulness required to establish liability for the privacy statutes or the intentionality required to establish liability for intrusion on seclusion.

General

General damages – *i.e.*, non-pecuniary, "pain and suffering" damages – are awarded at large. A party seeking general damages need not prove the actual number.[140]

For example, in cases of intrusion upon seclusion where there is no pecuniary loss, symbolic or moral damages may be awarded up to $20,000. In Jones, the Court awarded $10,000.[141] Proof of actual loss is not an element of the cause of action.[142]

Factors to be considered in determining exact quanta can include:

- the nature, incidence and occasion of the defendant's wrongful act;
- the effect of the wrong on the plaintiff's health, welfare, social, business or financial position;
- any relationship, whether domestic or otherwise, between the parties;
- any distress, annoyance or embarrassment suffered by the plaintiff arising from the wrong; and
- the conduct of the parties, both before and after the wrong, including any apology or offer of amends made by the defendant.[143]

138. *Ibid*, at paras. 12, 14.
139. *Karasik 2 supra*, footnote 122, at paras. 140-141.
140. *Shillington, supra*, footnote 99, at para. 66.
141. *Jones, supra*, footnote 11, at para. 75.
142. *Ibid*, at para. 74.
143. *Jones, supra*, footnote 11, at para. 81.

In cases involving public disclosure of private facts, in particular the non-consensual distribution of intimate images or intimate image abuse, the Court will have particular regard to the significant and long-lasting harm that sexually-based wrongdoing causes to human dignity.[144]

The Court will consider cases of sexual assault and battery by analogy, including:

- the circumstances of the assaults, their number, frequency, and how violent, invasive, and degrading they were;
- the circumstances of the defendant, including age and whether he or she was in a position of trust; and
- the consequences for the victim, including ongoing psychological injuries.[145]

In the *Jane Doe* cases, the Court awarded $50,000 in general damages.[146] In *Shillington* and in *L.D.S.*, the Court awarded $80,000 in general damages.[147]

Overall, the Courts appear inclined to require plaintiffs to show proof of actual compensable harm in privacy actions. In *Setoguchi*, Rooke J. said:[148]

> I believe that, similar to Québec, mutatis mutandis, the risk of a future injury developing – a hypothetical injury - is not an injury that can be compensated. This is different from real harm arising out of preventing further interference with [personal information]. [Citations omitted.]

Mental Distress

In assessing general damages, the question of damages for mental distress arises. It is not disputed that worry, inconvenience, and annoyance are not states of mental distress for which the law compensates.[149] However, the distress must rise to a compensable level.

In *Bourbonniere c. Yahoo! Inc.*, the Court held that transient embarrassment and inconveniences are of the nature of ordinary

144. *Shillington supra*, footnote 99, at paras. 89-90; *Jane Doe #1, supra*, footnote 82, at para. 53.

145. *Jane Doe #1, ibid*, at paras. 52-53; *Jane Doe #2, supra*, footnote 91, at paras. 128-129; *Shillington supra*, footnote 199, at para. 89.

146. *Jane Doe #1, ibid*, at para. 58; *Jane Doe #2, ibid*, at para. 139.

147. *L.D.S., supra*, footnote 99, at para. 103; *Shillington, supra*, footnote 99, at para. 97.

148. *Setoguchi*, *supra*, footnote 22, at para. 55.

149. *Mustapha v. Culligan of Canada Ltd.*, 2008 SCC 27, [2008] 2 S.C.R. 114, 293 D.L.R. (4th) 29 (S.C.C.), at para. 9.

annoyance, and do not constitute recoverable damages. The need to change a password at a higher frequency cannot give rise to a serious compensable loss claim.[150]

There was a similar outcome in a class action against the Investment Industry Regulatory Organization of Canada (IIROC) (under its French name): *Lamoureux v. Organisme canadien de reglementation du commerce des valeurs mobilieres* (*OCRCVM*).[151]

In February 2013, an IIROC inspector misplaced his unencrypted laptop on a train. The device, which was merely password-protected, contained personal information belonging to thousands of Canadian investors. It was never recovered. The Québec Superior Court dismissed the proceeding because Mr. Lamoureux had failed to establish any harm beyond those ordinary and everyday annoyances, which the law does not find compensable. The Quebec Court of Appeal dismissed the appeal, but leave to appeal has been filed to the Supreme Court of Canada.[152]

In *Evans*, the plaintiffs claimed damages for emotional suffering and inconvenience. The Court allowed the class proceeding to go ahead with damage of this kind as an issue, as the situation was unique. The plaintiffs' "personal financial records were distributed to third party criminals and where such confidential information has been used to steal their identity and commit fraud and has negatively affected their credit ratings."[153]

Aggravated and Punitive

A cybersecurity breach may also give rise to aggravated or punitive damages.

Aggravated damages may be awarded when the defendant's conduct has been high-handed or oppressive, increasing the Plaintiff's humiliation and anxiety. *Hill v. Church of Scientology of Toronto*,[154] and later public disclosure of private facts cases,[155]

150. 2019 QCCS 2624, 2019 CarswellQue 5830, EYB 2019-313513 (C.S. Que.), at paras. 37-44.

151. 2021 QCCS 1093, 333 A.C.W.S. (3d) 481, 2021 CarswellQue 3852 (C.S. Que.) at paras. 72-74, affirmed 2022 QCCA 685, 2022 CarswellQue 6143, EYB 2022-450059 (C.A. Que.). See also *Li c. Equifax inc.*, 2019 QCCS 4340, 312 A.C.W.S. (3d) 29, 2019 CarswellQue 9207 (C.S. Que.), affirmed *Equifax inc. c. Li*, 2018 QCCA 1560, 2018 CarswellQue 8411, EYB 2018-302319 (C.A. Que.), leave to appeal refused *Equifax Inc., et al. v. Daniel Li*, 2019 CarswellQue 1739, 2019 CarswellQue 1740 (S.C.C.), and *BourbonniÉre v. Yahoo! Inc.*, 2019 QCCS 2624, 2019 CarswellQue 5830, EYB 2019-313513 (C.S. Que.).

152. 2022 CarswellQue 13126 (S.C.C.).

153. *Evans, supra*, footnote 65, at para. 52.

establish that aggravated damages require a finding that the defendant was motivated by actual malice.

Punitive damages are awarded in accordance with the factors the Supreme Court set out in *Whiten v. Pilot Insurance Co*.[156] To attract an award of punitive damages, the misconduct must represent "a marked departure from ordinary standards of decent behaviour".[157]

How an organization responds to a data breach can make or break their defence to a punitive damages claim. In *Lamoureux*,[158] the Quebec Court of Appeal affirmed the lower court's decision to decline punitive damages because of the way that IIROC responded to the breach. The uncontradicted expert evidence established that IIROC applied best practices to the situation.[159] The expert concluded, among other things, that IIROC's response was in line with the guidelines of the National Institute of Standards and Technology in the event of cyber incidents.

Defendants involved in cyberbreach litigation should consider *Lamoureux* as guidance on how to respond to a data breach and consider whether expert evidence should be obtained to refute any arguments favouring punitive damages.

An organization's failure to learn from its mistakes and to prevent a repeat of cybersecurity breaches can render an award for punitive damages appropriate. In *Ari v. Insurance Corporation of British Columbia*,[160] an ICBC employee allegedly accessed the information of 78 customers, including names, addresses, driver's license numbers, vehicle descriptions and identification numbers, license plate numbers, and claims histories.[161] The illegally obtained information was used to target 13 of the customers with vandalism, arson, and shootings.[162]

The employee then provided the information to an acquaintance in a criminal organization.[163] The employee was charged under s.

154. (1995), [1995] 2 S.C.R. 1130, (*sub nom.* Manning v. Hill) 126 D.L.R. (4th) 129, 24 O.R. (3d) 865 (note) (S.C.C.), at para. 188.
155. *Shillington supra*, footnote 99, at para. 100.
156. 2002 SCC 18, [2002] 1 S.C.R. 595, 209 D.L.R. (4th) 257 (S.C.C.), at para. 113; *L.D.S., supra*, footnote 99, at para. 109; *Jane Doe #1, supra*, footnote 82, at para. 60; *Jane Doe #2, supra*, footnote 99, , at para. 140.
157. *Whiten v. Pilot Insurance Co*., 2002 SCC 18, [2002] 1 S.C.R. 595, 209 D.L.R. (4th) 257 (S.C.C.), at para. 36.
158. *Supra*, footnote 151.
159. 2022 QCCA 685, 2022 CarswellQue 6143, EYB 2022-450059 (C.A. Que.) at para. 23, affirming 2021 QCCS 1093, 333 A.C.W.S. (3d) 481, 2021 CarswellQue 3852 (C.S. Que.), at paras. 129-134.
160. 2019 BCCA 183, 27 B.C.L.R. (6th) 102, 305 A.C.W.S. (3d) 439 (B.C. C.A.).
161. *Ibid*, at para. 2.
162. *Ibid*, at para. 3.

342.1 of the *Criminal Code*. Once the breach was discovered, the plaintiff brought a proposed class action against the ICBC for the statutory tort of violation of privacy. The plaintiff alleged that ICBC was vicariously liable for the employee's wrongful acts.[164]

The Court certified the proceeding, but declined to certify, *inter alia*, the issue of punitive damages.[165] On appeal, the British Columbia Court of Appeal found the certification judge had erred on this point:[166]

> Rather than consider the past history of breaches of privacy by ICBC employees–the evidence supported that at least 7 employees have been terminated by ICBC between 2008 and 2011 for privacy breaches–the chambers judge considered the steps taken since the breach in this case was discovered. While laudable on ICBC's part, subsequent conduct is not the sole basis upon which punitive damages are determined. The chambers judge should have accepted as true the allegation that ICBC has a history of employees breaching private information. Instead, she judged the case on the merits on the evidence before her. That was an incorrect approach.

The appeal regarding punitive damages was allowed.

In Agnew-Americano, Glustein J. also certified the matter for punitive damages. The proposed representative plaintiff relied on the defendants' knowledge of previous hacking attempts, investigations, and audits, as well as their knowledge that they were particularly vulnerable to being hacked, and knew their systems were attractive to fraudsters. The punitive damages findings were not disturbed on appeal to the Divisional Court.[167]

Other

In exceptional circumstances, the disgorgement of profits by the wrongdoing party could be appropriate.[168]

In *Agnew-Americano*, Glustein J. allowed the claim of "restitutionary damages" to return fees paid to Equifax to proceed.[169] This finding was also not disturbed on appeal to the Divisional Court.[170]

163. *Ibid*, at para. 2.
164. *Ibid*, at para. 4.
165. *Ibid*, at para. 7.
166. *Ibid*, at para. 30.
167. *Owsianik, supra*, footnote 38, at para. 4.
168. Justice Glustein canvasses the law in *Agnew-Americano*, at para. 272ff.
169. *Agnew-Americano*, at paras. 280-286.
170. *Owsianik*, at para. 4.

Corporations or banks will incur incident response costs in response to a breach, choosing to offer free credit monitoring services to affected individuals, or to repay any monies stolen.[171] Defendants can be ordered to provide credit monitoring to affected individuals for a specified period if an affected individual requests the service as a remedy.[172]

That raises the question of whether the costs defendants pay as a result of cybersecurity attacks are recoverable through insurance. A decision of the New Jersey Superior Court provides some guidance.

In *Merck & Co. Inc. v. Ace American Insurance Company et al.*,[173] Merck brought a motion for partial summary judgment against its insurer Ace American. Ace had refused to cover losses and damages under an all-risks policy, resulting from the destruction or corruption of computer data and software because there was an exclusion given the source of the malware. Ace argued that because the "Notpetya" malware was an instrument of the Russian government, the hostile or warlike action by a government power exclusion clause applied. Merck argued that there were significant facts which showed it to be a form of ransomware.

The Court found that the exclusion clause did not apply. The Court found Merck's interpretation of the clause as only applying to traditional forms of warfare, and not cyber-based attacks to be reasonable. Merck's $1.4 billion-dollar business interruption losses resulting from the cyberattack were thus covered under the $1.75 billion all-risks policy.

While there is no comparable decision in Canada, in *Oliviera v. Aviva Canada Inc.*, the Ontario Court of Appeal confirmed that an insurer was not relieved of its duty to defend Norfolk General Hospital when an employee was alleged to have committed the tort of intrusion upon seclusion.[174]

171. *Kaplan, supra*, footnote 27, at para. 2; *Evans*, at para. 5.
172. *eHealth Saskatchewan, Re*, 2021 CarswellSask 12 (Sask. I.P.C.), at para. 197.
173. 2022 WL 951154 (N.J. Super. Law Div., 2022) (Trial Order).
174. *Oliveira v. Aviva Canada Inc. et al*, 2017 ONSC 6161, 73 C.C.L.I. (5th) 58, [2018] I.L.R. l-6011 (Ont. S.C.J.) at para. 57, affirmed *Oliveira v. Aviva Canada Inc.*, 2018 ONCA 321, 79 C.C.L.I. (5th) 65, 290 A.C.W.S. (3d) 169 (Ont. C.A.), at para. 3. See also *Demme v. Healthcare Insurance Reciprocal of Canada*, 2021 ONSC 2095, [2021] I.L.R. 6294, 331 A.C.W.S. (3d) 653 (Ont. S.C.J.), affirmed 2022 ONCA 503, 24 C.C.L.I. (6th) 1, 83 C.C.L.T. (4th) 1 (Ont. C.A.).

F. A Brief Note on Constitutional Litigation

This article addresses civil litigation. However, Canadian common law offers other modes of recourse, depending on the nature of the cybersecurity breach.

The first is criminal litigation, discussed above. The second is constitutional litigation. The Supreme Court of Canada has emphasized the quasi-constitutional status of privacy.[175] It has recognized three aspects of the right: personal privacy, territorial or spatial privacy, and informational privacy.

One most readily recognizes a cybersecurity breach as a breach of informational privacy, defined as "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated."[176]

Section 8 of the *Charter of Rights and Freedoms* guarantees everyone the right to be secure against unreasonable search or seizure.[177] A state seizure of personal information could conceivably give rise to a claim.

However, constitutional litigation has its limits. First, the *Charter* only applies to government actions. Second, damages are rarely awarded in *Charter* cases.[178]

Avoiding Liability, Mitigating Damage

Litigation offers the prospect of future redress for past harms. Potential defendants may avoid those harms, and the liability for them, *a priori* through prevention and prophylaxis, while, a *posteriori* when the harms do occur, defendants may (but plaintiffs must) mitigate the damage through well-designed and implemented incident response plans.

Since the litigation profile of cybersecurity breaches remains emergent in Canadian Common Law, no court has yet identified the prevention or mitigation factors that would suffice for defendants to avoid liability for breaches, and plaintiffs to satisfy their duty to mitigate. The Québec courts' *Lamoureux* decision serves as an initial

175. *Douez v. Facebook, Inc.*, 2017 SCC 33, [2017] 1 S.C.R. 751, 411 D.L.R. (4th) 434 (S.C.C.). at para. 59.

176. *R. v. Dyment*, [1988] 2 S.C.R. 417, 55 D.L.R. (4th) 503, 45 C.C.C. (3d) 244 (S.C.C.); *R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432, 244 D.L.R. (4th) 541 (S.C.C.), at para. 23.

177. *Pt. 1 of the Constitution Act, 1982, being Sched. B of the Canada Act*, 1982, c. 11 (U.K.).

178. *Schachter v. Canada*, [1992] 2 S.C.R. 679, 93 D.L.R. (4th) 1, 92 C.L.L.C. 14,036 (S.C.C.); *Hislop v. Canada (Attorney General)*, 2007 SCC 10, [2007] 1 S.C.R. 429, 278 D.L.R. (4th) 385 (S.C.C.), at para. 81.

beacon of guidance for liability avoidance in its acceptance of expert evidence regarding an organization's response to a data breach.

Otherwise, the law is a laggard on what prevention or mitigation steps it will consider sufficient to relieve a defendant from liability.

Technology and cybersecurity companies, specialists and consultants have developed and propagated protocols and practices to prevent breaches and mitigate the damage when they occur.

The details of such protocols and practices are the proper subject of a technical paper, not ours. However, they will likely form a basis for Canadian Common Law principles governing liability and damages from cybersecurity breaches. To that end, we offer a condensed overview of best practices for prevention and mitigation.

A. Guidance and Where to Find It

Cybersecurity civil litigators – plaintiff or defendant, Bar or Bench – will not lack for available guidance on cybersecurity prevention and mitigation, as this image demonstrates:

7.45 billion results. That abundance is one reason for our offering only an overview of best cybersecurity practices.

That same abundance, however, also means that guides and guidance are readily available to one and all. Thus, for example, no defendant in a cybersecurity breach action will be able to argue credibly that they could not have known what to do to avoid or mitigate the breach. The answers – 7.45 billion of them – lie in a simple Google search.

Of those answers, the ones the search engine first serves up are those of the federal government agency, the Canadian Centre for Cyber Security.

Given the governmental provenance of the Centre's guidance, there is every possibility that it will become, or at least inform, the standard to which Canadian courts will hold defendants in cybersecurity breach civil litigation. While we have crafted our own best practices outline below, we have relied on the Centre's *Baseline Cyber Security Controls For Small And Medium*

Organizations[179] as a template (and commend it to the reader as an authoritative source).[180]

B. Best Practices

According to the noted cybersecurity writer Brian Krebs, "the most important principle in cybersecurity defense that applies to both corporations and consumers: Assume you are compromised".[181]

Mr. Krebs' assumption is an important, if dire, starting point for cybersecurity resilience. It entails that best practices not concern themselves with breach prevention alone. They must also include breach response and repair, since prevention presumptively has failed or will fail, *per* Mr. Krebs.

Best practices, then, will (and must) fall into one of three broad categories:

1. Prevention
2. Detection
3. Response

Thus classified, the components of an organization's cybersecurity plan will take the following shape:

PREVENTION
• Identify and ensure compliance with cybersecurity laws in jurisdictions to which the organization may be subject
• Catalogue IT systems and assets, hardware and software

179. Canada, "Baseline cyber security controls for small and medium organizations" (2020 February) online: https://www.cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations, modified May 13, 2021, accessed July 14, 2022. The Guidance defines "small and medium organizations" as those with less than 499 employees (at para 2.1, OC.1). The best practices we derive from the Guidance apply equally to larger organizations, although the cybersecurity measures the larger organizations adopt will need to be of greater scale and scope.

180. In *Lamoureux, supra*, footnote 151, the Québec courts accepted the recommendations of the U.S. National Institute of Standards and Technology (NIST) as authoritative in validating IIROC's incident response. See Paul Cichonski, Tom Millar, TimGrance, Karen Scarfone, *Computer Security Incident Handling Guide,* NIST Special Publication 800-61, Revision 2, August 31, 2012, online, https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final, accessed August 7, 2022.

181. Brian Krebs, "What the Marriott Breach Says About Security", December 1, 2018, https://krebsonsecurity.com/2018/12/what-the-marriott-breach-says-about-security, accessed July 14, 2022.

PREVENTION
• Assess how the confidentiality, integrity, and availability of the IT systems and assets might be compromised or impaired
• Identify potential cyber threats
• Budget appropriately for cybersecurity
• Deploy sufficient and appropriate personnel, including outside providers, with proper responsibility and decision-making authority for IT security
• Have clear policies for the appointed personnel's exercise of their IT security authority, within organizational departments and across them
• Restrict network administrative access to appropriate personnel, with the minimum functionality necessary, and confine general user-level access to reduced threat activities
• Deploy an array of strong security tools that update and scan automatically
• Deploy strong controls for hardware and software
• Activate firewalls on devices within organizational networks, or implement alternative measures in place of the firewalls
• Encrypt all data
• Publish rules on ownership and network-related use of mobile devices
• Implement secure configurations for all devices within organizational networks, changing all default passwords, turning off unnecessary features, and enabling all relevant security features
• Implement two-factor authentication, and document all decisions not to do so
• Develop and enforce clear policies on password length, reuse, and security
• Provide mandatory cybersecurity awareness and training for all personnel who use the organization's networks
• Remove accounts and functionality for personnel that no longer need them
• Ensure adequate backup systems are in place, and that recovery mechanisms can effectively and efficiently restore these back-ups
• Consider cybersecurity insurance that includes coverage for incident response and recovery
• Test, verify, document, and audit all prevention measures regularly

DETECTION
• Maintain continuous cybersecurity measures and detection systems
• Ensure detection systems for hardware and software are up to date
• Enable automatic patching for all software and hardware. or establish full vulnerability and patch management practices
• Monitor detection systems actively, not passively
• Look for trouble
RESPONSE
• Publish a clear and thorough incident response plan that identifies an incident response team, authority of team members, collaboration protocols, and criteria for issue mitigation and resolution
• Include in the response plan contact information for internal and external parties, stakeholders, and regulators
• Ensure up-to-date hard copies of plan are available, in case digital copies are not accessible
• Ensure the response plan covers incidents of varying severity, including significant ones for which the organization will require outside help
• Run regular response plan exercises and drills
• Implement incident response plan, including containment procedures, as soon as possible
• Implement backup systems immediately pending restoration of network health
• Issue notices to affected parties
• Issue notices required by statute
• Contact authorities who may be able to assist with recovery
• Consider legal avenues for emergency redress, such as injunctions
• Ensure regular clear, effective, regular communication with parties, stakeholders, and regulators

C. The Litigation Implications of Best Practices

The business case for cybersecurity best practices is obvious. Cybersecurity breaches impose heavy costs.

To begin, there are the immediate monetary costs. In Canada, the estimated average cost of a breach in 2021 (including, but not limited to ransomware) was $6.35 million.[182]

Then there are the wider, more long-term costs. These include:

- loss of trust amongst clientele
- business interruption, including employee downtime
- business data loss
- insurance costs
- systems and data reconstruction
- regulatory liability, for example in the securities or health sectors

Lastly, there are the civil liability implications we have been discussing in this article. Adopting cybersecurity best practices can inoculate parties whose systems suffer a breach in two ways.

1. **Damage mitigation and avoidance**: Best practices can help avoid liability in the first place. When well-implemented, they can help reduce detection and resolution times for breaches. Cybersecurity breaches are a process, not an event.[183] The more quickly a breach can be identified and neutralized, the more likely any harms, and thus any damage, may be avoided or at least mitigated.
2. **Standard of care:** Well-designed and executed practices and protocols may suffice by themselves to meet the requisite standard of care in the causes of action we have identified above. Recall that the standard of care (in negligence, but the principle is of general application) is reasonability, not perfection.[184] A defendant with a strong cybersecurity plan could well be found to have taken reasonable steps to avoid and respond to a breach. Such a finding would enable the defendant to avoid liability, for punitive damages in particular (see *Lamoureux*, *supra*).

182. Canadian Centre for Cyber Security, *Cyber threat bulletin: The ransomware threat in 2021*, https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-ransomware-threat-2021, accessed June 13, 2022.

183. A frequently cited model for the process of cybersecurity breaches is the 7-step Lockheed Martin Cyber Kill Chain framework: *The Cyber Kill Chain*, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html, accessed July 14, 2022.

184. *Waterway Houseboats Ltd. v. British Columbia*, 2020 BCCA 378, 40 C.E.L.R. (4th) 1, 10 M.P.L.R. (6th) 1 (B.C. C.A.), at para. 374.

To these two potential effects of developing and executing a sound cybersecurity plan, one must add the plaintiffs' general duty to take reasonable steps to mitigate their damages. A plaintiff who failed to do the latter, faced with a defendant who has done the former will likely find themselves challenged to command a generous remedy from the Courts.

Conclusion: a *Donoghue v. Stevenson* Moment

Civil litigation and technology are at a *Donoghue v. Stevenson* moment.

Scottish and English Common Law responded to Mary Donoghue's plight of finding the snail in her ginger beer by creating what has evolved into modern-day negligence law. To the suggestion that Ms. Donoghue was without a remedy under the Common Law principles of the time, Lord Atkin famously responded:

> I do not think so ill of our jurisprudence as to suppose that its principles are so remote from the ordinary needs of civilized society and the ordinary claims it makes upon its members as to deny a legal remedy where there is so obviously a social wrong.

In the past two decades in Canada, technology and its uses have evolved from a niche adjunct to a pervasive necessity. Whether dealing with businesses, governments, or family members, it has become, paraphrasing Lord Atkin (above), one of the ordinary needs of civilized society that makes ordinary claims upon its members.

In *Donoghue v. Stevenson*, the common law barely (3 to 2) but firmly responded to the advent of the manufacture and distribution of ginger beer (and much else) and its attendant harms with a new remedy that re-shaped tort law and brought it into the 20th Century. Similarly, we can expect that Canadian common law will respond to the advent of technology and the harms it has ushered in with a new remedy that will further expand tort law and plant it firmly in the 21st Century.