DIRECT AND VICARIOUS LIABILITY FOR TORT CLAIMS INVOLVING VIOLATION OF PRIVACY

Barbara von Tigerstrom

The growth of actions for violation of privacy presents a significant risk for defendants and an opportunity for civil claims to provide a mechanism for accountability. However, several key issues that would determine the scope of liability remain unsettled. In most cases, courts have concluded that the existence of statutes dealing with personal information does not exclude the possibility of civil actions, which is important given the limits of statutory remedies. Negligence claims in this context may face issues regarding the duty of care, particularly where the defendant is a public authority, and proof of injury, given that recovery for harms such as stress or economic loss is limited. Therefore, the availability of statutory or common law privacy torts, which do not require proof of actual damage, is very important, but the elements of these torts are evolving and may be difficult to prove against an organization where the main perpetrator of the violation is an individual employee or third party. Vicarious liability for a breach of privacy by a "rogue" employee is possible, but will depend on whether the facts show that the employer organization materially increased the risk of the violation. The current state of the law raises questions about the ability of these claims to effectively provide compensation or deterrence, but in the absence of legislative reform, the progressive development of the law on some of these issues could help to clarify and expand the options available to address ongoing threats to privacy.

L'augmentation du nombre des poursuites pour atteinte à la vie privée représente un risque important pour les défendeurs et une occasion pour les poursuites civiles d'offrir un mécanisme de reddition de compte. Cependant, plusieurs éléments fondamentaux qui détermineraient la portée de la responsabilité demeurent incertains. Dans la plupart des cas, les tribunaux ont conclu que l'existence des lois portant sur les renseignements personnels n'exclut pas la possibilité de poursuites civiles, ce qui est important étant donné les limites des recours statutaires. Les poursuites fondées sur la négligence dans ce contexte pourraient se heurter à des questions liées à l'obligation de diligence, plus particulièrement lorsque le défendeur est une entité publique, et à la preuve du préjudice, étant donné le caractère limité du recouvrement au titre des préjudices tels que le stress et les pertes économiques. Par conséquent, la possibilité d'invoquer des recours statutaires ou de common law pour atteinte

* Professor, University of Saskatchewan. The author gratefully acknowledges funding from the Foundation for Legal Research, excellent research assistance by Arfa Hussein and Shawna Sparrow (JD students, University of Saskatchewan) and helpful comments from the anonymous reviewers.

à la vie privée, lesquels n'exigent pas la preuve de l'existence de dommages réels, est très importante. Toutefois, les éléments de ces recours sont en pleine évolution et pourraient être difficiles à établir à l'égard d'une organisation au sein de laquelle le principal auteur de la violation est un employé individuel ou un tiers. La responsabilité du fait d'autrui pour une atteinte à la vie privée du fait d'un employé « rebelle » est possible, mais dépendra de la question de savoir si les faits révèlent que l'organisation qui l'emploie a sensiblement augmenté les risques de violation. L'état actuel du droit soulève la question de la capacité de ces demandes à assurer adéquatement l'indemnisation ou la dissuasion. Cependant, en l'absence d'une réforme législative, l'évolution progressive du droit sur certaines de ces questions pourrait aider à clarifier et à multiplier les options disponibles pour régler les menaces constantes qui pèsent sur la vie privée.

Contents

1. Introduction 540

2. Tort Claims Relating to Breach of Privacy 541

A) Relationship Between Civil Claims and Other Remedies 543

B) Negligence Liability and Compensable Harm 549

C) Direct Liability for Statutory or Common Law Privacy Torts 554

D) Vicarious Liability for Breaches of Privacy 557

3. Conclusion 562

1. Introduction

Privacy breaches of various kinds are increasingly the subject of public attention and concern. High-profile breaches have led to calls for improved accountability and oversight.[1] Civil claims could be one mechanism for accountability, and there is a growing body of case law dealing with claims for violations of privacy, either through negligence or intentional conduct. In many of these cases, there is an organization (e.g., a company or public body) that could bear direct and/or vicarious liability for the violation, which could make some claims viable where they would not be if only an individual defendant is involved. An organization could face significant

[1] See e.g. Office of the Privacy Commissioner of Canada, "Appearance Before the Standing Committee on Access to Information, Privacy and Ethics to Discuss the Study About the Breach of Personal Information Involving Cambridge Analytica and Facebook: Opening Statement by Daniel Therrien, Privacy Commissioner of Canada" (17 April 2018), online: *Office of the Privacy Commissioner of Canada* <www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2018/parl_20180417/>.

liability if a number of individuals are affected, even if the damages claimed by each individual are fairly small.

The growth of such actions, given the combination of vicarious liability, class proceedings, and a broader range of claims,[2] presents a significant risk for defendants and an opportunity for those who see civil claims as an important means of seeking accountability. In the United States, however, the track record of information privacy claims has recently been described as "stunningly poor,"[3] and some of the same difficulties are likely to exist in Canada. In addition, to date Canadian class actions have been certified, and in some cases settled, but not yet decided on their merits,[4] which means that several key issues that would determine the scope of liability have yet to be fully considered or decided. The aim of this article is to identify and explore those issues, with a view to examining the potential tort liability of organizations for various types of privacy breaches and assessing the current state of the law.

2. Tort Claims Relating to Breach of Privacy

The landscape for privacy claims in common law Canada has been evolving rapidly since the Court of Appeal for Ontario recognized a common law tort of intrusion upon seclusion in 2012,[5] adding an important new option for claimants. Depending on the jurisdiction and the facts of each case, relevant tort claims can include negligence and either common law or statutory privacy claims. Intrusion upon seclusion is now well established in Ontario and has been recognized, or at least not ruled out, as a potential claim in several other Canadian jurisdictions.[6] The related tort of publishing or giving publicity to private facts has also been applied or recognized as a potential claim in a few cases.[7] In four provinces, a statutory tort of violation

---

2 Omar Ha-Redeye, "Class Action Intrusions: A Development in Privacy Rights or an Indeterminate Liability?" (2015) 6:1 Western J Leg Studies 1 at 13 [Ha-Redeye]; Barry Glaspell & Daniel Girlando, "The Rise of Personal Health Information Class Actions" (2015) 11:1 Can Class Action Rev 49 at 69 [Glaspell & Girlando].

3 Julie E Cohen, "Information Privacy Litigation as Bellwether for Institutional Change" (2017) 66:2 DePaul L Rev 535 at 536 [Cohen].

4 Glaspell & Girlando, *supra* note 2 at 49.

5 *Jones v Tsige*, 2012 ONCA 32, 108 OR (3d) 241 [*Jones*].

6 *Grant v Winnipeg Regional Health Authority*, 2015 MBCA 44, 385 DLR (4th) 346 [*Grant*]; *Trout Point Lodge Ltd v Handshoe*, 2012 NSSC 245, 320 NSR (2d) 22; *Capital District Health Authority v Murray*, 2017 NSCA 28, 278 ACWS (3d) 242; *Rancourt-Cairns v Saint Croix Printing and Publishing Company Ltd*, 2018 NBQB 19, 2018 NBBR 19; *Hynes v Western Regional Integrated Health Authority*, 2014 NLTD(G) 137, 1109 APR 138 [*Hynes*]; *R v John Doe*, 2016 FCA 191, [2016] FCJ No 695 [*John Doe*].

7 *Jane Doe 464533 v ND*, 2016 ONSC 541, 128 OR (3d) 352, rev'd on other grounds 2017 ONSC 127, 276 ACWS (3d) 261 [*Doe 464533*]; *Halley v McCann*, 2016 CanLII 58945 (Ont Sm Cl Ct) [*Halley*]; *John Doe*, *supra* note 6.

of privacy has been available for many years,[8] and a distinct tort of non-consensual distribution of intimate images has more recently been added in some provinces.[9] This discussion focuses on common law and statutory tort claims, but other options may be available in certain cases, including breach of confidence, breach of fiduciary duty, breach of contract, and claims under consumer protection legislation.[10] In addition, as further discussed below, there is limited provision for damages under some federal and provincial personal information legislation.

The range of potential claims means that one or more of them may be available in different fact scenarios. These include inadvertent breaches through the loss or transmission of personal information, such as where a laptop, memory key, or other data storage device is lost,[11] or where errors in mailing or other transmission lead to personal information being disclosed.[12] They also include external breaches, where a third party gains unauthorized access to an organization's computer system, which might or might not have been prevented by better safeguards.[13] Other cases involve an internal breach due to unauthorized access ("snooping") or disclosure

---

8 *Privacy Act*, RSBC 1996, c 373 [*Privacy Act* (BC)]; *Privacy Act*, RSS 1978, c P-24 [*Privacy Act* (SK)]; *Privacy Act*, CCSM c P125 [*Privacy Act* (MB)]; *Privacy Act*, RSNL 1990, c P-22 [*Privacy Act* (NL)].

9 *The Intimate Image Protection Act*, CCSM c I87, s 11; *Protecting Victims of Non-Consensual Distribution of Intimate Images Act*, RSA 2017, c P-26.9, s 3. In Saskatchewan, *The Privacy Amendment Act*, SS 2018, c 28, which received royal assent in May 2018, will create an equivalent provision by amendment of the *Privacy Act* (SK), *supra* note 8, and in Nova Scotia, s 6(3) of the *Intimate Images and Cyber-protection Act*, SNS 2017, c 7, proclaimed in July 2018, allows a court to order payment of general, special, aggravated, or punitive damages or an accounting for profits where a person has distributed an intimate image without consent.

10 Additional claims are available in Quebec based on articles 35 and 36 of the *Civil Code of Québec*, CQLR c CCQ-1991, and article 5 of the Quebec *Charter of Human Rights and Freedoms*, CQLR c C-12.

11 See e.g. *Rowlands v Durham Region Health*, 2012 ONSC 3948, 217 ACWS (3d) 779 [*Rowlands*] (lost memory key); *Sofio c Organisme canadien de réglementation du commerce des valeurs mobilières (OCRCVM)*, 2014 QCCS 4061, EYB 2014-241279, aff'd 2015 QCCA 1820, [2014] JQ no 10718 [*Sofio*] (lost laptop); *Condon v R*, 2015 FCA 159, [2015] FCJ No 803 [*Condon*] (lost hard drive).

12 See e.g. *John Doe*, *supra* note 6 (envelopes sent by Health Canada with return address for medical marijuana access program); *Speevak v Canadian Imperial Bank of Commerce*, 2010 ONSC 1128, 93 CPC (6th) 195 (misdirected faxes); *Mazzonna c DaimlerChrysler Financial Services Canada Inc/Services financiers DaimlerChrysler inc*, 2012 QCCS 958, EYB 2012-203721 [*Mazzonna*] (loss of data tape).

13 See e.g. *Drew v Walmart Canada Inc*, 2017 ONSC 3308, 10 CPC (8th) 182 [*Drew*]; *Zuckerman c Target Corporation*, 2017 QCCS 110, EYB 2017-275197 [*Zuckerman*]; *Agnew-Americano v Equifax Canada*, 2018 ONSC 275, 288 ACWS (3d) 27 [*Agnew-Americano*]; *Tucci v Peoples Trust Company*, 2017 BCSC 1525, [2017] BCWLD 5559 [*Tucci*].

by an employee of the organization.[14] Depending on the nature of the breach, some combination of negligence, violation of privacy, or both may be appropriate causes of action against an organization and/or its employee. Where the information of a number of individuals is involved, certain types of privacy breaches may lend themselves to class proceedings.[15]

Potential issues arise for each type of claim in certain scenarios. First, there is the preliminary issue of how civil claims relate to other types of oversight mechanisms and remedies. Second, negligence claims, in particular, may face issues regarding the defendant's duty of care, the applicable standard of care, or the plaintiff's injury. Common law or statutory claims for violation of privacy avoid these issues, but raise other questions, including the requirement for wilful or intentional conduct. Finally, the question of when an organization will be vicariously liable for the tortious conduct of an employee may be contentious where the breach involves unauthorized conduct by a "rogue" employee. Each of these issues will be explored in the sections that follow.

A) Relationship Between Civil Claims and Other Remedies

Throughout Canada there is legislation governing the collection, use, and disclosure of personal information in the public and private sectors, which include complaint mechanisms and sometimes other remedies, to address breaches and other issues. Although some plaintiffs include the breach of relevant statutes among their claims,[16] it is well established that in Canada, breach of statute is not a distinct cause of action.[17] Instead, a breach of statute can be used as evidence of negligence;[18] conversely, compliance with statutory or regulatory standards can be evidence that the standard of care has been met.[19] Therefore, compliance or noncompliance with a statute such as the *Personal Information Protection and Electronic Documents Act*

---

14 See e.g. *Evans v The Bank of Nova Scotia*, 2014 ONSC 2135, 55 CPC (7th) 141 [*Evans*]; *Jones*, *supra* note 5; *Ari v Insurance Corporation of British Columbia*, 2015 BCCA 468, 392 DLR (4th) 671 [*Ari v ICBC* (CA)]; *Hynes*, *supra* note 6. See also *Doucet v The Royal Winnipeg Ballet*, 2018 ONSC 4008, 2018 CarswellOnt 10757, regarding the taking and dissemination of intimate photographs by an employee of the organization.

15 Adrian Lang & Lesley Mercer, "Privacy Breaches: The New Frontier in Class Actions" (2015) 10:1 Class Action Defence Q 1 at 2: "Unfortunately for defendants, privacy breaches are often ripe for certification due to the fact that data breaches often affect groups of similarly situated people (i.e., who have had similar types of personal data misplaced and/or disclosed to the same unauthorized third parties) as a result of the same data breach".

16 See e.g. *Hynes*, *supra* note 6 at paras 31–33; *Drew*, *supra* note 13 at para 8.

17 *Canada v Saskatchewan Wheat Pool*, [1983] 1 SCR 205, 143 DLR (3d) 9.

18 *Ibid*.

19 *Ryan v Victoria (City)*, [1999] 1 SCR 201, 168 DLR (4th) 513 [*Ryan*].

("*PIPEDA*")[20] may be used by defendants or plaintiffs, respectively, to bolster their positions in a civil action. Although statutory obligations can therefore inform a negligence analysis, plaintiffs risk having their claims dismissed if they explicitly claim a breach of statute as a cause of action or even if a negligence claim is too closely tied to statutory obligations.[21]

In some cases, breach of an applicable statute may give rise to a claim for damages under the statute itself; this is the case for *PIPEDA*,[22] the private sector *Personal Information Protection Act* ("*PIPA*") in British Columbia ("BC") and Alberta,[23] the *Personal Health Information Protection Act* ("*PHIPA*") in Ontario,[24] and public sector legislation in Quebec.[25] Such provisions, along with the oversight mechanisms available under these and other statutes, have led some defendants to argue that information and privacy legislation "occupies the field" and excludes the possibility of civil liability, leaving only legislative remedies. This argument was rejected in relation to *PIPEDA* in *Jones v Tsige*,[26] and then in relation to *PHIPA* in *Hopkins v Kay*.[27] In *Jones*, the Court of Appeal for Ontario quickly concluded that *PIPEDA* did not preclude the recognition of a common law cause of action for intrusion upon seclusion, stating that "it would take a strained interpretation to infer from [*PIPEDA* and Ontario public sector and health information legislation] a legislative intent to supplant or halt the development of the common law in this area."[28] In *Jones*, the plaintiff's claim was against a "rogue employee" rather than the organization that was subject to *PIPEDA* (the bank), so *PIPEDA* would be unlikely to provide a remedy in her case.[29] The fuller consideration in *Hopkins* examined the provisions of *PHIPA* to determine whether it implicitly excluded the court's jurisdiction and other claims dealing with the same subject matter. Although *PHIPA* does provide a comprehensive set of rules and some remedies, the Court noted that the Commissioner's investigation of complaints is discretionary, that provisions in the Act explicitly recognize the potential for court proceedings dealing with matters falling within its scope, and that the common law claim

---

20 SC 2000, c 5 [PIPEDA].

21 See e.g. *Ari v ICBC* (CA), *supra* note 14; *Cook v Insurance Corporation of British Columbia*, 2014 BCSC 1289, [2014] BCWLD 5607 [*Cook v ICBC*], discussed below.

22 PIPEDA, *supra* note 20, s 16.

23 *Personal Information Protection Act*, SBC 2003, c 63, s 57 [PIPA (BC)]; *Personal Information Protection Act*, SA 2003, c P-6.5, s 60 [PIPA (AB)].

24 *Personal Health Information Protection Act*, SO 2004, c 3, Schedule A, s 65 [PHIPA].

25 *Act Respecting Access to Documents Held by Public bodies and the Protection of Personal Information*, CQLR c A-2.1, s 167 [Quebec Access and Protection Act].

26 *Jones*, *supra* note 5.

27 *Hopkins v Kay*, 2015 ONCA 112, 380 DLR (4th) 506 [*Hopkins*].

28 *Jones*, *supra* note 5 at para 49 [footnotes omitted].

29 *Ibid* at para 50.

is independent of and distinct from the statute. These observations led to the conclusion that *PHIPA* was not intended to be an exhaustive code.[30]

Allowing civil claims to coexist with statutory oversight mechanisms is critical to providing compensation to affected individuals. Most public sector information and privacy statutes have no provision for an award of damages,[31] only recommendations or orders aimed at changing organizations' behaviour. Where damages are provided for, there are significant limitations on their availability. A decision by the relevant commissioner or a conviction under the statute is a prerequisite to seeking damages.[32] Furthermore, some statutes only allow damages for "actual harm"[33] or for "loss or injury" suffered as a result of the breach,[34] which may be difficult to establish in many cases,[35] as will be discussed further below. There is no such restriction in *PIPEDA*, but an award of damages is discretionary and will be made only in "egregious" situations,[36] in order to uphold the objects and values of the legislation and deter future breaches.[37] Damage awards are thus fairly rare; where they have been given, most have been modest.[38] It could certainly be argued (as it was in *Jones* and *Hopkins*[39]) that all of this reflects policy choices of Parliament and the legislatures, intended to limit the remedies available for breach of these statutory obligations. Accepting this argument would, however, leave us with no effective remedy or other accountability for many privacy breaches, and its implications for public sector defendants—against whom no damages or other concrete remedies are available under most statutes—are troubling. It may be possible for courts to strike a balance by

---

30 *Hopkins*, *supra* note 27 at paras 29–62.

31 Quebec is the exception: see Quebec Access and Protection Act, *supra* note 25, s 167.

32 PIPEDA, *supra* note 20, s 14 (which also restricts applications to the Court to breach of certain listed provisions of the Act); PIPA (BC), *supra* note 23, s 57(1); PIPA (AB), *supra* note 23, s 60(1); PHIPA, *supra* note 24, s 65(1).

33 PIPA (BC), *supra* note 23, s 57(1), (2); PHIPA, *supra* note 24, s 65(1), (2). In Ontario, PHIPA provides for damages of up to $10,000 for "mental anguish," but only as an additional claim where the harm suffered is the result of a wilful or reckless contravention or offence: PHIPA, *supra* note 24, s 65(3).

34 PIPA (AB), *supra* note 23, s 60(1), (2).

35 Ha-Redeye, *supra* note 2 at 10.

36 *Randall v Nubodys Fitness Centres*, 2010 FC 681 at para 55, 371 FTR 180.

37 *Nammo v TransUnion of Canada Inc*, 2010 FC 1284 at para 76, 379 FTR 130 [*Nammo*]. See also *Blum v Mortgage Architects Inc*, 2015 FC 323 at paras 19–20, 476 FTR 299.

38 See *Henry v Bell Mobility*, 2014 FC 555 at para 22, 456 FTR 180, summarizing past PIPEDA damage awards, which (with one exception) have ranged from $0 to 5,000. There are no reported cases in which damages have been awarded under the other statutes.

39 See *Jones*, *supra* note 5 at para 48; *Hopkins*, *supra* note 30 at para 27.

leaving open the potential for civil claims by using procedural mechanisms to address duplicative proceedings on a case-by-case basis.[40]

Since *Jones*, other courts have reached the conclusion that *PIPEDA* does not exclude the possibility of civil claims,[41] nor does the federal *Privacy Act*.[42] Plaintiffs can therefore bring tort claims for breaches of privacy, even when they fall within the scope of public or private sector information and privacy legislation. Some recent decisions from BC appear to go against this trend. In one, the argument that *PIPA* "has occupied the field" was accepted as excluding a claim against a pharmacy (while the claim against the pharmacist was allowed to proceed, since it was grounded in distinct common law and equitable duties of the pharmacist as a health professional).[43] One decision considering the *Freedom of Information and Protection of Privacy Act* ("*FIPPA*") found it to be an exhaustive code, "to the exclusion of the civil courts for matters under that statute,"[44] and in another, *FIPPA* and its remedies provided one of several policy reasons to deny a duty of care in a negligence claim.[45] Although these decisions appear to be inconsistent with the general trend of allowing common law remedies to parallel statutory regimes, it is notable that the claims in these cases relied

---

40 For example, the courts will need to address *res judicata* issues and consider concerns about wasted resources from duplicate proceedings: see Liam O'Reilly, "Getting to Damages in the Health Information Privacy Context: Is the Cost Worth the Damage?" (2016), online (pdf): <admin.nibbler.io/v1/AUTH_ca1f094bfd8b4ceea3a48b9c95409073/canlii_production/uploads/opinion/file/42318/Liam_O_Reilly__Getting_to_Damages_in_the_Health_Information_Privacy_Context__Is_the_Cost_Worth_the_Damages.pdf>. See also *Agostino v Bank of Montreal*, 2014 FC 961, 2014 CF 961 (proceedings in Quebec courts and in Federal Court under PIPEDA relating to the same breach; Federal Court proceedings stayed).

41 *Chandra v CBC*, 2015 ONSC 5303 at paras 29–38, 24 CCLT (4th) 330; *Tucci*, *supra* note 13 at paras 57–89.

42 *Romana v The Canadian Broadcasting Corporation*, 2016 MBQB 33 at paras 21–26, 325 Man R (2d) 196 (regarding a claim under the *Privacy Act* (MB), *supra* note 8). See also *Condon v R*, 2014 FC 250 at paras 109–15, 450 FTR 216, rev'd 2015 FCA 159, 474 NR 300, where the point was not directly argued but raised and rejected in the course of discussing whether a class proceeding was the preferable procedure to deal with claims regarding a breach by a federal agency.

43 *McIvor v MLK Pharmacies Ltd*, 2016 BCSC 2249 at paras 31–33, [2017] BCWLD 162 [*McIvor*].

44 *Cook v ICBC*, *supra* note 21 at para 70. The claim for the statutory tort of violation of privacy was allowed to proceed, although matters properly under FIPPA would have to be separated at a later stage: *ibid* at para 165.

45 *Ari v ICBC* (CA), *supra* note 14 at paras 53–63.

heavily on statutory duties even when asserting distinct causes of action,[46] and this appears to have affected the analysis.[47]

Furthermore, these decisions must be seen in the broader context of others from the BC courts, which have been more resistant to accepting common law privacy torts than their counterparts elsewhere. A series of decisions have stated that there is no common law cause of action for violation of privacy in BC, and although most of these statements are in *obiter*, they have been repeated enough times to be accepted as definitive.[48] One frequently cited decision properly refused to accept a Supreme Court of Canada decision[49] based on the Quebec *Charter of Human Rights and Freedoms*[50] as creating a cause of action in BC.[51] It has since been cited for the simple proposition that there is no common law tort of invasion of privacy in the province.[52] Even as courts elsewhere have begun to recognize a common law tort, BC courts have continued to deny its existence in that province.[53] More recent decisions suggest that the main reason for this is the BC *Privacy Act*, which provides a statutory cause of action.[54] Courts in other jurisdictions have accepted that the statutory and common law causes of action may coexist,[55] but provisions in the Privacy Acts of the other three provinces—to which there is no equivalent in BC—explicitly leave open the possibility of other claims.[56]

---

46 *McIvor*, *supra* note 43 at para 8; *Cook v ICBC*, *supra* note 21 at paras 40–41, 165; *Ari v ICBC* (CA), *supra* note 14 at paras 2, 12.

47 Subsequent decisions have read the reasons in *Cook* and *Ari* in this light: see *McIvor*, *supra* note 43 at para 16 and *Tucci*, *supra* note 13 at para 136.

48 See e.g. *Ari v ICBC* (CA), *supra* note 14 at para 9: "It is common ground that in British Columbia there is no common law cause of action for breach of privacy".

49 *Aubry c Éditions Vice Versa Inc*, [1998] 1 SCR 591, 157 DLR (4th) 577.

50 *Supra* note 10.

51 *Hung v Gardiner*, 2002 BCSC 1234 at para 110, 45 Admin LR (3d) 243, aff'd on other grounds 2003 BCCA 257, 227 DLR (4th) 152.

52 *Bracken v Vancouver Police Board*, 2006 BCSC 189 at para 28, [2006] BCWLD 2505 [*Bracken*]; *Demcak v Vo*, 2013 BCSC 899 at para 8, [2013] BCWLD 4879 [*Demcak*]; *Ari v Insurance Corporation of British Columbia*, 2013 BCSC 1308 at para 63, 54 BCLR (5th) 197 [*Ari v ICBC* (SC)]. See also *Mohl v University of British Columbia*, 2009 BCCA 249 at para 13, 271 BCAC 211 [*Mohl*].

53 *Demcak*, *supra* note 52 at para 8; *Ari v ICBC* (SC), *supra* note 52 at paras 62–65; *Ladas v Apple Inc*, 2014 BCSC 1821 at para 76, [2014] BCWLD 7259.

54 *Foote v Canada (AG)*, 2015 BCSC 849 at para 116, [2015] BCWLD 3633; *Tucci*, *supra* note 13 at paras 152–55.

55 *Hynes*, *supra* note 6; *Hagan v Drover*, 2009 NLTD 160, 291 Nfld & PEIR 193; *Grant*, *supra* note 6.

56 *Privacy Act* (SK), *supra* note 8, s 8(1); *Privacy Act* (MB), *supra* note 8, s 6; *Privacy Act* (NL), *supra* note 8, s 7(1). See e.g. *Hynes*, *supra* note 6 at para 25.

In Alberta, the situation is less clear and the stakes are higher given the absence of a statutory tort for violation of privacy in that jurisdiction, leaving only the limited provision for damages under *PIPA*. Although the arguments that succeeded in *Jones*, *Hopkins*, and other cases would seem to be persuasive in relation to the Alberta *PIPA*, a few decisions in that province have questioned the existence of a common law claim for breach of privacy. None of these fully consider and decide the point, and they are weak authority to the extent that they rest at least in part on what appear to be questionable readings of earlier cases[57]—or on authority from BC,[58] where distinct considerations apply. The position in Alberta thus remains uncertain, but there is no reason in principle why a common law tort should not be recognized there, coexisting with *PIPA* and public sector legislation.

Finally, even when tort claims are available, plaintiffs' abilities to recover may be affected by statutory provisions limiting liability. Some federal and provincial/territorial information and privacy legislation includes provisions that limit or exclude liability for conduct contrary to the legislation if it is done in good faith.[59] On one hand, the existence of such provisions can help to convince a court that the legislation implicitly leaves open the possibility of parallel civil claims,[60] but on the other, they may bar some of those claims given the difficulty of proving bad faith.[61] Notably, however, there

---

[57] For example, *Martin v General Teamsters, Local Union No 362*, 2011 ABQB 412 at paras 45–46, [2011] AWLD 4093, cites *Bank of Montreal v Cochrane*, 2010 ABQB 541, [2011] AWLD 204 [*Cochrane*] for the proposition that there is no common law claim for breach of privacy, but omits part of the relevant passage from *Cochrane*, from which it appears the court did not actually make any clear statement on the existence of a common law claim. More recently, the Court in *Al-Ghamdi v Alberta*, 2017 ABQB 684 at para 160, [2018] AWLD 499 referred to a breach of privacy claim as "controversial," citing *Scherf v Nesbitt*, 2009 ABQB 658 at para 24, 18 Alta LR (5th) 248 [*Nesbitt*] which briefly referred, in *obiter*, to a possible claim for breach of privacy, and *Pinder v Canada (Minister of the Environment)*, 2015 FC 1376 at paras 107–08, 262 ACWS (3d) 214 (aff'd on other grounds 2016 FCA 317, 274 ACWS (3d) 321), which specifically stated that there was no *general* claim for breach of privacy, apart from the intrusion upon seclusion tort recognized in Ontario, which was not applicable on the facts of that case.

[58] See *Cochrane*, *supra* note 57 at para 7; *Nesbitt*, *supra* note 57 at para 24, citing *Mohl*, *supra* note 52.

[59] See e.g. PIPA (AB), *supra* note 23, s 57; *Privacy Act*, RSC 1985 c P-21, s 74; *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165, s 30 [FIPPA], s 73; *Freedom of Information and Protection of Privacy Act*, RSO 1990, c F.31, s 62(2); PHIPA, *supra* note 24, s 71.

[60] See *Hopkins*, *supra* note 27 at para 41.

[61] See e.g. *Bracken*, *supra* note 56 at paras 50, 58, where the immunity provision in s 73 of the BC FIPPA, *supra* note 59, protected one of the defendants from liability. But see *Ari v ICBC* (CA), *supra* note 14 at para 30, where section 73 was found not to apply because the disclosure was not in good faith.

is no such provision in *PIPEDA*.[62] Even where they do exist, their impact depends on how they are interpreted: the Federal Court of Appeal recently held that the immunity provision in the federal *Privacy Act* did not, given its wording, act to protect the Crown against actions in negligence and breach of confidence.[63]

Although some uncertainty remains, current trends in the jurisprudence indicate that public- and private-sector personal information legislation can provide limited remedies and, more importantly, does not appear to exclude the possibility of civil claims for conduct that would also be a breach of statutory obligations. Exactly how statutory mechanisms and civil claims will interact is among the many issues that remain to be resolved as more cases work their way through the courts. The need to update and expand statutory remedies may also become more pressing depending on the outcome of civil claims, which face a number of obstacles that are explored in the following sections.

B) Negligence Liability and Compensable Harm

A negligence claim in the context of a breach of privacy will need to establish all of the usual elements of a negligence action: "(1) that the defendant owed him a duty of care; (2) that the defendant's behaviour breached the standard of care; (3) that the plaintiff sustained damage; and (4) that the damage was caused, in fact and in law, by the defendant's breach."[64] Any of these could be contentious depending on the facts of a particular case. Where the defendant is a public authority, there are potential obstacles to establishing a duty of care. For example, the Court of Appeal for BC held that the Insurance Corporation of British Columbia ("*ICBC*"), a public body, did not owe a duty of care to the claimants because of several policy considerations. As mentioned above, the Court saw *FIPPA* as a comprehensive legislative framework for public sector privacy concerns, and this weighed against finding a duty of care.[65] It

---

62 PIPEDA, *supra* note 20, s 22 protects the Commissioner from civil or criminal liability for exercising his or her powers under the Act in good faith.

63 The provision, s 74, states: "Notwithstanding any other Act of Parliament, no civil or criminal proceedings lie against the head of any government institution, or against any person acting on behalf or under the direction of the head of a government institution, and no proceedings lie against the Crown or any government institution, for the disclosure in good faith of any personal information *pursuant to* this Act, for any consequences that flow from that disclosure, or for the failure to give any notice required under this Act if reasonable care is taken to give the required notice" [emphasis added]. The Court held that the wording "pursuant to" qualified the scope of the immunity and it was therefore not relevant to civil claims that did not rest on the *Privacy Act*: *John Doe*, *supra* note 6 at paras 41–43.

64 *Mustapha v Culligan of Canada Ltd*, 2008 SCC 27 at para 3, [2008] 2 SCR 114 [*Mustapha*].

65 *Ari v ICBC* (CA), *supra* note 14 at paras 53–63.

also pointed to concerns about indeterminate liability and the fact that the allegedly negligent conduct could be characterized as policy decisions[66]—two common obstacles to negligence claims involving public authorities.[67] Concerns about indeterminate liability were arguably misplaced in this case; the alleged duty of care was not to the public at large (to all of whom statutory duties are owed under *FIPPA*), but rather to the plaintiff as a customer of *ICBC*. Particularly given the narrow understanding of indeterminate liability recently urged by the Supreme Court of Canada,[68] it is difficult to see how this constitutes an indeterminate class. The so-called "immunity" for policy decisions may or may not be an issue depending on the specific allegations of negligent conduct. In this case, the Court characterized the claim as being directed at "the adequacy of security measures that *ICBC* undertook, as a matter of *policy*," under the relevant section of *FIPPA*, rather than the way the measures were "actually carried out."[69]

The standard of care that is expected of organizations in this context may also be a significant issue and is yet to be fully explored. Clearly, not every failure to prevent a security breach or even every unintended disclosure will be considered negligent, since the standard is reasonable care, not perfection. In the absence of jurisprudence specific to privacy breaches, we can look to basic principles for guidance. In any negligence case, the reasonableness of the defendant's conduct depends on the seriousness and probability of the risks involved, as well as the costs of preventing or mitigating the risks. This suggests that carelessness in mailing, faxing, or disposing of personal information, where errors can be fairly easily prevented and could have significant consequences, is more likely to be found negligent than inadequate computer security measures, where mitigating risks may be more burdensome and costly, and standards are constantly changing. Customary practice and industry standards are likely to be important guides, especially for more technical matters, subject always to the proviso that following a common practice can still in some cases be considered unreasonable. As mentioned above, compliance or lack of compliance with statutory obligations may also inform the standard of care; they will carry more weight if the statutory provisions are specific and relevant to the risks involved,[70] which is arguably the case here. Some of the statutory obligations relating to protection of personal information refer in general terms to "reasonable" or "appropriate" measures[71]—concepts that parallel a

---

66 *Ibid* at paras 50–52.

67 See e.g. *Cooper v Hobart*, 2001 SCC 79, [2001] 3 SCR 537; *R v Imperial Tobacco Canada Ltd*, 2011 SCC 42, [2011] 3 SCR 45.

68 *Deloitte & Touche v Livent Inc (Receiver of)*, 2017 SCC 63 at paras 42–45, [2017] 2 SCR 855.

69 *Ari v ICBC* (CA), *supra* note 14 at para 52 [emphasis in original].

70 *Ryan*, *supra* note 19 at paras 39–40.

71 See e.g. FIPPA, *supra* note 59; PIPEDA, *supra* note 20, Sch 1, cl 4.7.

negligence approach, balancing the magnitude of the risk against availability and cost of preventive measures and the value of the activity.[72] There is a rich body of privacy commissioners' decisions and guidance documents interpreting these provisions that could inform a court's analysis. Finding the right balance in determining the standard of care—expecting neither too much nor too little of organizations that are responsible for personal information—will be important to ensuring fairness for both parties.

Another generally applicable concern, which may be a significant obstacle for some plaintiffs, is their ability to establish that they sustained damage that is recognized as compensable. Unlike the common law and statutory privacy torts, negligence is not actionable per se and requires proof of harm, preferably an injury to person or property. As others have noted, this is likely to be an issue for many claims involving breach of privacy.[73] Problems may arise if the harm is purely in the form of economic loss, if threatened harms have not yet manifested, or if the impact does not reach the threshold that the law recognizes as compensable.

Where the harm is purely economic, such as money spent on credit monitoring or money lost through fraud, plaintiffs must contend with the restrictions on recovery for pure economic loss in Canadian negligence law. Pure economic loss is only recoverable in certain specific categories of cases.[74] Some of these may be useful in specific fact scenarios: for example, negligent misrepresentation could apply where the defendant has made representations about its measures to protect personal information and negligent performance of a service may be applicable in some cases.[75] If the new category of negligent misrepresentation to a third party gains recognition,[76] it may assist plaintiffs in certain situations.[77] However,

---

72 *Various Claimants v WM Morrisons Supermarket Plc*, [2017] EWHC 3113 (QB) at paras 68–69, [2018] IRLR 200 [*Morrisons*].

73 Jennifer A Chandler, "Negligence Liability for Breaches of Data Security" (2008) 23:2 Banking & Finance L Rev 223 at 232 [Chandler]; Gideon Emcee Christian, "A New Approach to Data Security Breaches" (2009) 7:1 Can J L & Tech 149 at 168 [Christian]; Lisa Talbot, Molly Reynolds & Eliot Che, "Canadian Privacy Class Actions at the Crossroads" (2015) 11:1 Can Class Action Rev 31 at 41 [Talbot, Reynolds & Che]. In some cases, it may also be difficult to prove that the injury was caused by the defendant's negligence: see Chandler at 235–38.

74 *Winnipeg Condominium Corporation No 36 v Bird Construction Co*, [1995] 1 SCR 85 at para 12, 121 DLR (4th) 193.

75 Chandler, *supra* note 73 at 248–49.

76 *Haskett v Equifax Canada Inc* (2003), 63 OR (3d) 577 (CA), (*sub nom Haskett v Trans Union of Canada Inc*) 224 DLR (4th) 419.

77 See e.g. *Nammo*, *supra* note 37; *Parmar v Royal Bank of Canada*, 2016 ABQB 439, [2016] AWLD 3578; *Dimov v Equifax Canada Co*, 2017 NSSM 1, 2017 CarswellNS 108. However, in these cases the complaint is not necessarily that personal information was

many claims for negligent disclosure or negligent failure to prevent use or disclosure will fall outside the recognized categories. It remains possible to argue that another category should be created,[78] but this would be a novel claim with uncertain prospects.

Another problem is that the damage resulting from a breach may not be immediately evident and the possibility of future harm—e.g., exposing individuals to the *risk* of fraud or identity theft—may not be recognized as a distinct compensable injury.[79] Where the damages claimed are for stress and anxiety from the breach itself or from worrying about potential harms, there is a risk that a negligence claim will fail. Although proof of a recognized psychiatric illness is no longer required to establish mental injury in a negligence claim,[80] it remains well established that the injury suffered "must be serious and prolonged and rise above the ordinary annoyances, anxieties and fears that people living in society routinely, if sometimes reluctantly, accept."[81] Some privacy breaches certainly cause serious mental injury,[82] but in other cases the result is better described as stress, annoyance, or inconvenience, which would fall below the threshold required. Likewise, it is not clear that the time and expense involved in preventing or mitigating losses (e.g., by checking or changing bank or credit card accounts or monitoring accounts for fraudulent activity) could be recognized as compensable damages.[83]

Courts will generally give plaintiffs the benefit of the doubt at a preliminary stage, so some claims have been certified or survived motions to dismiss even where damages are questionable. Given the nature of the analysis at these preliminary stages, the courts focus on whether the pleadings set out the nature of damages claimed,[84] leaving the question of whether the evidence will support a claim for compensable damages as a

---

disclosed, but that reports were inaccurate, so they are not directly concerned with breach of privacy.

78 Chandler, *supra* note 73 at 249–50; Christian, *supra* note 73 at 181–83.

79 This has been a significant barrier in US cases: see Cohen, *supra* note 3 at 539–43; Chandler, *supra* note 73 at 232, 238–40; Christian, *supra* note 73 at 167; Talbot, Reynolds & Che, *supra* note 73 at 42–43.

80 *Saadati v Moorhead*, 2017 SCC 28, [2017] 1 SCR 543.

81 *Mustapha*, *supra* note 64 at para 9.

82 See e.g. *LAM v JELI*, 2008 BCSC 1147, [2008] BCJ No 1612; *Doe 464533*, *supra* note 7.

83 Christian, *supra* note 73 at 166.

84 See *Condon*, *supra* note 11 at paras 20–22; *John Doe*, *supra* note 6 at paras 49–51, where the Court held that it was sufficient for the purposes of certification of class proceedings that the nature of the damages claimed were set out in the pleadings, read generously, as long as they were not "negligible inconveniences nor entirely speculative" (*ibid* at para 51).

matter to be determined at trial.[85] This allows claims to go forward and in some cases, reach settlement: for example, in *Rowlands v Durham Region Health*, where the loss of a USB key containing personal information caused anxiety and distress but the probability of misuse of the information was low, the weakness of the plaintiffs' claim for damages in negligence was a significant factor in finding a settlement to be in the class members' best interests.[86] In other cases, it may be sufficiently clear from the pleadings that the claim cannot succeed. Several decisions have held that stress and inconvenience associated with the exposure of claimants' personal information through loss or a security breach are not sufficient damages to support a class action.[87]

A novel argument could be made that increasing individuals' risk or making them vulnerable to harms such as fraud or identity theft should be recognized as a form of injury in itself. It has been suggested that, like individuals exposed to toxic substances who may be able to recover the cost of medical monitoring, victims of privacy breaches—especially data breaches that expose them to financial risks—should be compensated for the time and cost of monitoring their financial affairs.[88] A recent decision of the United Kingdom Supreme Court may provide some support for this line of argument. In *Dryden v Johnson Matthey Plc*, the Court unanimously held that plaintiffs who had developed "platinum sensitisation" as a result of their employer negligently exposing them to platinum salts could claim in negligence for associated financial losses.[89] Platinum sensitisation does not cause any symptoms, but puts an individual at risk of developing an allergy if further exposed to platinum, which caused the claimants to lose current and future employment opportunities. Lady Black (for the Court) rejected an argument that platinum sensitisation only amounted to a *risk* of injury,[90] and held that it was an actionable injury because it was a physical

---

85 See e.g. *Hynes*, *supra* note 6, where the plaintiffs claimed in negligence for unspecified damages for "distress, humiliation, anger, upset, anguish, shock, fear of identity theft, uncertainty as to how information was used, confusion … [and] feeling of vulnerability" (at para 27); in allowing the claim to go forward, Goodridge J noted that, depending on the evidence at trial, there may be some class members who had suffered no compensable harm (at para 29).

86 *Rowlands*, *supra* note 11 at paras 16–23. The settlement allowed class members who could show proof of financial harm to recover compensation, but ultimately no class member made such a claim: see Glaspell & Girlando, *supra* note 2 at 59.

87 *Zuckerman*, *supra* note 13 at para 69; *Mazzonna*, *supra* note 12; *Sofio*, *supra* note 11.

88 Chandler, *supra* note 73 at 240–43; Christian, *supra* note 73 at 168–69; Cohen, *supra* note 3 at 545–46.

89 [2018] UKSC 18, [2018] 3 All ER 755.

90 *Ibid* at paras 42–43.

change that diminished the claimants' physical capacity.[91] The financial loss suffered by the claimants was from lost earnings associated with this injury, not pure economic loss, and could therefore be claimed.[92] At first glance, this decision seems to support an argument that causing claimants to be in a condition that makes them vulnerable to further injury could be recognized as a harm in itself, and the claimants should be able to recover for financial loss associated with avoiding further injury (e.g., avoiding certain types of work, in *Dryden*, or credit monitoring, in a data breach case). The critical distinguishing feature, of course, is that in the *Dryden* case there is a physical injury involved, whereas in the data breach case there is generally no present impact on the claimant's person, only a risk of possible future economic loss. A stronger argument could be made if there is some mental injury that could be analogized to the physical injury in *Dryden*.

In summary, a negligence claim faces obstacles at the duty of care and damages stages, as well as uncertainty relating to the standard of care. A generous approach to some of these issues could expand the scope of liability to some degree, but it seems likely that in many cases negligence claims may not play a meaningful role in providing compensation or accountability. Further clarification of the standard of care would provide useful guidance, but perhaps not much deterrent effect on defendants' conduct if claims are not viable for other reasons. Other causes of action will therefore be important as alternatives or supplements to a negligence claim.

C) Direct Liability for Statutory or Common Law Privacy Torts

In most of Canada, statutory and/or common law privacy torts may be available, all of which are actionable without proof of actual damage. However, the elements of these torts may cause problems of their own in some cases. The uncertain status of some common law tort claims is the first hurdle. Although the tort of intrusion upon seclusion is now established in Ontario, it has not been definitively recognized elsewhere.[93] The tort of publication of private facts (or giving publicity to private facts) would be more appropriate in some fact scenarios, but its recognition and elements remain unclear. It has been applied in lower court decisions in Ontario,[94] but rejected as inapplicable to specific facts[95] or outright as a matter of principle[96] in other decisions. Where it has been applied or acknowledged as a possible claim, interpretation of its elements, particularly what constitutes

91 *Ibid* at para 40.

92 *Dryden*, *supra* note 93 at para 44.

93 See above note 6.

94 *Doe 464533*, *supra* note 7; *Halley*, *supra* note 7.

95 *John Doe*, *supra* note 6 at para 56.

96 *Chandra v CBC*, *supra* note 41 at para 49.

"publicity," varies.[97] These points will be clarified as claims work their way through the courts, but this will take some time and in the meantime, there is considerable uncertainty about the scope for such claims.

Both the common law tort of intrusion upon seclusion and the statutory tort under the *Privacy Act* require an element of intent that may be difficult to meet in some fact situations. Intrusion upon seclusion requires:

> [F]irst, that the defendant's conduct must be *intentional, within which I would include reckless*; second that the defendant must have invaded, without lawful justification, the plaintiff's private affairs or concerns; and third, that a reasonable person would regard the invasion as highly offensive causing distress, humiliation or anguish.[98]

Under the *Privacy Act* in BC, Saskatchewan, and Newfoundland and Labrador, it is "a tort, actionable without proof of damage, for a person, *wilfully* and without claim of right, to violate the privacy of another."[99] In this context, wilfulness has been interpreted as requiring "an intention to do an act which the person doing the act knew or should have known would violate the privacy of another person."[100] Other decisions have understood wilful to mean intentional or not accidental.[101] Therefore, both the statutory and common law torts require at least intentional or reckless conduct. In some cases, the defendant organization's conduct is more appropriately described as careless or negligent, such as when personal information is disclosed through improper disposal or an "administrative error"; this will not cross the threshold of being wilful or even reckless.[102] In other cases, the organization itself has not disclosed personal information, but has allowed

---

97 Compare: *John Doe*, *supra* note 6 at paras 55–56; *Doe 464533*, *supra* note 7 at para 47; *Halley*, *supra* note 7 at para 25.

98 *Jones*, *supra* note 5 at para 71 [emphasis added].

99 *Privacy Act* (BC), *supra* note 8, s 1(1) [emphasis added]. The language in *Privacy Act* (SK), *supra* note 8, s 2 and *Privacy Act* (NL), *supra* note 8, s 3(1) is virtually identical. Only Manitoba's statute differs in that there the tort is committed when a person "substantially, unreasonably, and without claim of right, violates the privacy of another person": *Privacy Act* (MB), *supra* note 8, 2(2).

100 *Hollinsworth v BCTV* (1998), 59 BCLR (3d) 121, [1999] 6 WWR 54 (CA) at para 29. This definition has been cited in many other decisions, including *St Pierre v Pacific Newspaper Group Inc and Skulsky*, 2006 BCSC 241 at para 49, [2006] BCWLD 2759; *Watts v Klaemt*, 2007 BCSC 662 at para 16, 71 BCLR (4th) 362.

101 *Duncan v Lessing*, 2018 BCCA 9 at para 86, 420 DLR (4th) 99; *Peters-Brown v Regina District Health Board* (1995), 136 Sask R 126 (QB), [1996] 1 WWR 337, aff'd (1996), 148 Sask R 248, [1997] 1 WWR 638 (CA).

102 See *John Doe*, *supra* note 6 at para 58; *Cole v Prairie Centre Credit Union Ltd*, 2007 SKQB 330 at paras 41–45, [2008] 1 WWR 115, respectively. See also Nicole Krueger, "Public Sector Privacy Breaches: Should British Columbians Have a Cause of Action for Damages Under the Freedom of Information and Protection of Privacy Act?" (2018) 23 Appeal 149 at 154–57 [Krueger].

it to be accessed and/or disclosed by a third party or by an employee. In such cases, it may be questionable whether its conduct can be described as intentional or, indeed, whether the organization itself has actually committed an intrusion or violation, which would be required for either a common law or statutory violation of privacy claim. The potential liability for privacy torts in some of these cases will depend on how strictly these elements are applied.

For example, where a defendant allegedly did not provide adequate security, allowing unauthorised access to personal information by an unknown third party, the judge stated that "it may be a stretch to call the disclosure here reckless … [or] to say that the defendant invaded the plaintiff's private affairs, as that was done by a third party," but allowed the action to go forward.[103] In another class action, involving computer software that allegedly made users' personal information vulnerable to hackers, it was again held that the intrusion upon seclusion claim was not "doomed to fail," given that the tort was still evolving.[104] It was argued that the defendant (Lenovo) putting the software onto claimants' laptops, "allowing private information to be sent to unknown servers," was itself an intrusion.[105] On the statutory tort of violation of privacy, the defendant argued that there was no "*actual* violation of anyone's privacy," since there was no evidence that anyone's information had actually been appropriated.[106] This argument was rejected by Justice Belobaba, who took the view that "[t]he risk of unauthorized *access* to private information is itself a concern even without any *actual* removal or actual theft," analogizing this to a peephole that allowed someone to look into another's bathroom, which could be considered a violation of privacy "even if the peephole was not being used at any particular time."[107]

In a later decision involving competing class actions relating to the Equifax security breach, one party attempted to distinguish the Lenovo decision on the basis that Lenovo had taken a specific, intentional action (installing the software),[108] whereas Equifax had allegedly only permitted an outside party to access information. In Justice Glustein's view, however, the intrusion upon seclusion claim could be viable in both cases; in both, the defendant had allegedly exposed the claimants to a known risk,[109] and "[i]f a 'peephole' analogy were to be applied … a court could find on the pleadings that the Equifax Defendants recklessly permitted a peephole to

103 *Tucci*, *supra* note 13 at para 152.

104 *Bennett v Lenovo*, 2017 ONSC 1082 at para 23, 2017 CarswellOnt 2314.

105 *Ibid* at para 20.

106 *Ibid* at para 27 [emphasis in original].

107 *Ibid* [emphasis in original].

108 *Agnew-Americano*, *supra* note 13 at paras 148–49.

109 *Ibid* at paras 146, 152.

be established."[110] Similarly, a court could find that the statutory tort of violation of privacy applies to a defendant who "wilfully permits hackers to access their network to obtain personal information" of its customers.[111] These views have yet to be tested at trial, however, and a recent decision of the Federal Court—approving settlement of a class action involving loss of a hard drive containing personal information—commented that in the absence of evidence that the information on the hard drive had been accessed, the plaintiffs would not have been able to prove that an intrusion upon seclusion actually occurred.[112]

The situation of an internal breach by a "rogue employee" who accesses or discloses personal information without proper authority is similar in that the direct liability of the organization would be in allowing this unauthorized access or disclosure to occur. It could, for example, be argued that the employer's failure to establish safeguards against unauthorised access constitutes a wilful violation of privacy.[113] The difference, as compared to cases involving third parties, is that vicarious liability may provide an alternative argument in the case of a breach by an employee.

D) Vicarious Liability for Breaches of Privacy

The doctrine of vicarious liability allows an employer to be held liable for torts committed by an employee within the scope of employment.[114] Vicarious liability, as a distinct claim and a form of strict liability, is independent of a claim for direct liability in negligence or for violation of privacy by the employer organization. It is therefore particularly important in cases of internal breaches (i.e. access or disclosure by an employee), because it could be hard to establish direct tort liability where the organization itself arguably did not commit the violation, and might not even have been negligent in allowing it to occur. Apart from the obstacles to any negligence claim, discussed above, unauthorized access or disclosure is a risk in any system where employees have access to personal information,[115] and "the hardest vulnerability to guard against [is] that of a person with authorised access behaving in a criminal manner."[116] Some of these breaches can be prevented, but the security of a system cannot be guaranteed without impractical and unduly intrusive measures.[117]

---

110 *Ibid* at para 151.

111 *Ibid* at para 165.

112 *Condon v Canada*, 2018 FC 522 at paras 28–31, 2018 CarswellNat 2769.

113 *Hynes*, *supra* note 6 at para 19.

114 *Bazley v Curry*, [1999] 2 SCR 534, 174 DLR (4th) 45 [*Bazley* cited to SCR].

115 *Morrisons*, *supra* note 72 at para 79.

116 *Ibid* at para 76.

117 *Ibid* at para 108.

Vicarious liability can therefore be critical to proving a remedy for affected plaintiffs, but risks unfairness to defendants in holding them responsible for breaches they could not reasonably have prevented—a familiar tension in cases involving vicarious liability for unauthorized or illegal conduct. The accepted test for vicarious liability for employees' tortious conduct is the "'Salmond' test, which posits that employers are vicariously liable for (1) employee acts authorized by the employer; or (2) unauthorized acts so connected with authorized acts that they may be regarded as modes (albeit improper modes) of doing an authorized act."[118] An employee negligently carrying out his or her duties, thereby putting personal information at risk, falls under the first branch of the Salmond test; in this scenario, if a viable negligence claim could be made out against the employee, vicarious liability of the employer would be likely to follow. Vicarious liability is possible but less certain in cases involving an intentional breach that is contrary to the employer's express aims and policies but nevertheless could be argued as having been committed "within the scope of employment."[119] Unauthorized access or disclosure falls under the second branch of the Salmond test, which is often much more difficult.

In *Bazley v Curry*, the Supreme Court of Canada set out the approach to be used in such cases. Where there is no clear precedent, courts should consider "whether the wrongful act is *sufficiently related* to conduct authorized by the employer" and whether there is a "significant connection between the *creation or enhancement of a risk* and the wrong that accrues therefrom," since this will determine whether the imposition of vicarious liability will be consistent with the policy considerations of providing "an adequate and just remedy" and deterrence.[120] In the context of intentional torts, factors relevant to the connection between the wrong and the employer's creation or enhancement of the risk include:

(a) the opportunity that the enterprise afforded the employee to abuse his or her power;

(b) the extent to which the wrongful act may have furthered the employer's aims (and hence be more likely to have been committed by the employee);

(c) the extent to which the wrongful act was related to friction, confrontation or intimacy inherent in the employer's enterprise;

---

118 *Bazley*, *supra* note 114 at para 10.

119 This is a common scenario in privacy breaches involving personal health information: see Glaspell & Girlando, *supra* note 2 at 57.

120 *Ibid* at para 41 [emphasis in original].

(d) the extent of power conferred on the employee in relation to the victim;

(e) the vulnerability of potential victims to wrongful exercise of the employee's power.[121]

The application of this test should be sensitive to the underlying policy considerations and "focus on whether the employer's enterprise and empowerment of the employee materially increased the risk" of the tortious conduct and resulting harm.[122]

Canadian courts have quite sensibly held that the question of vicarious liability for violation of privacy or intrusion upon seclusion should not be determined in preliminary proceedings and needs to be considered with a full "factual matrix" at trial,[123] and as yet there is no clear Canadian precedent on this point.[124] The most extensive discussion is in *Evans v The Bank of Nova Scotia*, where Justice Smith applied the test from *Bazley* to the claim of vicarious liability of the bank for unauthorized disclosure of customers' information by an employee and found that it was not plain and obvious that the claim would not succeed.[125] The employee was a mortgage administration officer who had access to "highly confidential customer information," which he admitted disclosing to third parties who used it for fraudulent purposes.[126] Most of the factors from *Bazley* pointed toward the imposition of vicarious liability:

> 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. The release of customers' confidential information by Wilson to third parties did not further the employer's aim of generating profits on good loans. Also, Wilson's wrongful acts were not related to friction, or confrontation inherent in the Bank's enterprise, but they were related to his necessary intimacy with the customers' personal and financial information. 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.[127]

---

121 *Ibid* at para 41.

122 *Ibid* at para 46.

123 *Ari v ICBC* (CA), *supra* note 14 at para 28. See also *Hynes*, *supra* note 6 at para 20.

124 Glaspell & Girlando, *supra* note 2 at 57.

125 *Evans*, *supra* note 14 at para 30.

126 *Ibid* at paras 2–3.

127 *Ibid* at para 22.

This analysis suggests a fairly broad scope for vicarious liability where an employee has and abuses access to confidential personal information; authorizing the employee to access and use the information creates the opportunity for tortious conduct relating to the information, gives the employee power over the information and its subjects that can be abused, creates a type of intimacy, and makes the individual subjects of the information vulnerable to this abuse. In *Bazley*, Justice McLachlin (as she then was) drew the following analogy: "To require or permit an employee to touch the client in intimate body zones may enhance the risk of sexual touching, just as permitting an employee to handle large sums of money may enhance the risk of embezzlement or conversion."[128] Similarly, we might say that permitting or requiring an employee to handle personal information materially increases the risk of a violation or intrusion involving that information. Some cases, like *Evans*, are close enough to the established line of cases holding employers vicariously liable for employees' theft or fraud that a persuasive case can be made for vicarious liability. In others, like cases involving personal health information, the vulnerability of victims in relation to the collection or disclosure of this sensitive information can be said to weigh in favour of vicarious liability.[129]

It might, however, be argued that the fact that an employee has access to personal information as part of his or her duties should not be enough to justify imposing vicarious liability. In cases involving other intentional torts, mere opportunity has not been considered sufficient and courts have looked closely at the nature of the employee's assigned duties and how they relate to the risk of tortious conduct.[130] In the first English decision on vicarious liability for a deliberate unauthorized disclosure, *Various Claimants v WM Morrisons Supermarket Plc*, the employee who disclosed the personal information of other employees was a senior IT internal auditor who, by virtue of his role, "would frequently be expected to gain access to and use" sensitive personal information and was trusted to do so.[131] Although some of the relevant acts were done outside working hours, off-site, and using personal computer equipment, Justice Langstaff found that there was "an unbroken thread that linked his work to the disclosure."[132] The data had been "deliberately entrusted" to the employee, rather than being "merely something to which work gave him access."[133] The employee's assigned role was specifically to receive, store, and then disclose the data, and he

---

128 *Bazley*, supra note 114 at para 45.

129 Ha-Redeye, *supra* note 2 at 12.

130 See e.g. *EB v Order of the Oblates of Mary Immaculate in the Province of British Columbia*, 2005 SCC 60, [2005] 3 SCR 45; *Jacobi v Griffiths*, [1999] 2 SCR 570 at para 45, 164 DLR (4th) 71.

131 *Morrisons*, *supra* note 72 at para 15.

132 *Ibid* at para 183.

133 *Ibid* at para 184.

had received it "acting as an employee" when he copied it.[134] Although the later disclosure was unauthorized and was intended to harm the employer, given the nature of the employee's role, the tort was committed as part of activity taken on behalf of the employer.[135] This was sufficient to establish vicarious liability for a breach of data protection legislation or for a breach of confidence or misuse of private information.[136]

Determinations of vicarious liability are "heavily fact-sensitive,"[137] and until more cases are decided, it will be difficult to predict what will be sufficient to establish the "significant connection" that is required between the creation and enhancement of risk and an employee's tortious conduct involving personal information. In the *Morrisons* decision, a strong case could be made given that the employee's role specifically involved dealing with large amounts of confidential information. In other cases, an employee's access to personal information may be more incidental than central to his or her role, and the determination will be more difficult. Broader imposition of vicarious liability will serve the objectives of compensation and deterrence, but courts will still need to weigh all of the relevant factors to find that the employer materially increased the risk of a violation in order to justify imposing liability.

Another question that arises in this context is whether there are certain types of claims for which vicarious liability should not be imposed. Courts in BC and Newfoundland have held that it is not plain and obvious that a claim of vicarious liability for violation of privacy under the *Privacy Act* could not succeed.[138] The Court of Appeal for BC distinguished its earlier decision in *Nelson v Byron Price & Associates Ltd*,[139] on which the defendant relied to argue that there should be no vicarious liability under a statute that deals with an intentional wrong.[140] *Nelson* involved a complaint under the provincial *Human Rights Code*,[141] ("the *Code*") and the wording of the *Code*—which allowed for an award of aggravated damages against a "person who contravened" the *Code*—was interpreted not to have been intended to allow for vicarious liability of the employer for the discriminatory conduct of an employee.[142] Similar reasoning has been used to deny vicarious liability

---

134 *Ibid* at paras 185–86.

135 *Ibid* at para 193.

136 *Ibid* at para 194.

137 *Ibid* at para 181.

138 *Ari v ICBC* (CA), *supra* note 14 at para 26; *Hynes*, *supra* note 6 at para 20.

139 (1981), 122 DLR (3d) 340, 27 BCLR 284 (CA) [*Nelson*].

140 *Ari v ICBC* (CA), *supra* note 14 at para 21.

141 RSBC 1979, c 186.

142 *Ari v ICBC* (CA), *supra* note 14 at para 22, citing *Nelson*, *supra* note 139 at paras 17–18.

for discrimination under other human rights legislation.[143] However, the Court held that although section 1(1) of the *Privacy Act* required a violation of privacy to be committed "wilfully," there was "no language (as there was in *Nelson*) that clearly limits a plaintiff to recovery of damages from the person identified in s. 1(1)."[144] Furthermore, given that vicarious liability has been imposed for other forms of intentional conduct, "[t]o the extent that s. 1(1) of the *Privacy Act* requires deliberate wrongdoing, it is not *per se* incompatible with vicarious liability."[145]

Other decisions also support the proposition that vicarious liability should not necessarily be excluded for a statutory cause of action. An Ontario court held that vicarious liability could apply to a statutory remedy for misrepresentation under securities legislation,[146] relying on authorities from the Supreme Court of Canada[147] and the House of Lords.[148] The House of Lords had held that vicarious liability should generally apply unless it was expressly or impliedly excluded by the relevant statute.[149] This authority was applied in *Morrisons* to find that there could be vicarious liability for violations of the *Data Protection Act* by an employee.[150] In coming to this conclusion, Justice Langstaff rejected "overstated" arguments about the potential for excessive liability (noting that this was the first case in the Act's 20-year history to consider vicarious liability for its breach),[151] and emphasized that the *Data Protection Act*'s purpose—"to provide greater protection of the rights of data subjects"—would be furthered by allowing additional liabilities.[152] These arguments should have some resonance in the Canadian context.

3. Conclusion

Determining the extent of organizations' liability is important in practical terms, since the odds of plaintiffs recovering meaningful compensation will be greater if there is a defendant organization that will bear direct or vicarious liability, rather than an individual or unknown third party. For defendant

---

143 *Robichaud v Canada*, [1987] 2 SCR 84, 40 DLR (4th) 57; *Janzen v Platy Enterprises Ltd*, [1989] 1 SCR 1252, 59 DLR (4th) 352.

144 *Ari v ICBC* (CA), *supra* note 14 at para 25.

145 *Ibid* at para 25.

146 *Allen v Aspen Group Resources Corporation*, 2012 ONSC 3498, [2012] OJ No 2924.

147 *Strother v 3464920 Canada Inc*, 2007 SCC 24, [2007] 2 SCR 177, where the majority held that vicarious liability could be imposed for a breach of fiduciary duty under provincial partnership legislation.

148 *Majrowski v Guy's and St Thomas' NHS Trust*, [2006] UKHL 34, [2007] 1 AC 224.

149 *Ibid*.

150 *Morrisons*, *supra* note 72 at paras 153–59.

151 *Ibid* at para 158.

152 *Ibid* at para 159.

organizations, it is also significant for predicting their potential exposure, particularly when facing class actions, and guiding their development of appropriate practices and procedures. The current state of the law is difficult to evaluate, since it is still at an early stage of development,[153] with many of the reported decisions only being preliminary. However, based on this (admittedly selective) review of issues, there are reasons to believe that the law is not meeting some basic objectives very well.

The patchwork of causes of action available in different jurisdictions and the evolving state of the law create complexity and uncertainty, particularly where plaintiffs reside in different parts of Canada. This is not ideal from the point of view of either plaintiffs or defendants, since it is difficult to predict when an action is viable and what liability a defendant will face. To a large extent, this is an inevitable result of the slow process of the law's development. Greater clarity will come with time, but we must also consider whether the law should just be allowed to develop through the gradual process of successive court decisions, or whether some type of legislative intervention is desirable.

The adequacy of the law's potential to provide compensation to affected individuals is questionable. It is certainly positive that, generally speaking, the existence of statutory mechanisms has not been taken to exclude the option of civil claims. It is quite appropriate that compensation will vary—or, in some cases, be denied altogether—depending on the facts of a particular case.[154] However, the limits on compensable injuries in negligence claims leave some plaintiffs who have suffered what we should recognize as real harms—financial loss, stress, and lost time, not to mention the real but intangible wrong that a violation entails—without a remedy. That would not be such a serious concern if the other potential claims were adequate to fill the gap, but each of the alternatives has significant limitations. Several of the statutory damages provisions have the same limited scope and all of them have other restrictions; common law or statutory torts for violation of privacy allow compensation without proof of damage, but may not be available in all jurisdictions and are not a good fit for all scenarios. Where the source of a breach is the deliberate conduct of an employee, vicarious liability may provide a remedy, but its scope remains unclear. Where there is an unknown third party involved, the organization holding the personal information would often be the only source of compensation and its liability may be difficult to establish.

The existing law is also arguably inadequate from the point of view of deterrence. Even when claims are successful or settlements are reached,

---

153 See e.g. Talbot, Reyolds & Che, *supra* note 73 at 45.

154 See Glaspell & Girlando, *supra* note 2 at 65–68.

there is little sign of this having an impact on organizations' practices, as privacy breaches continue to occur on a regular basis. The deterrent impact of liability is difficult to evaluate empirically, but the fact that liability is uncertain and fairly modest (relatively speaking) suggests that it is unlikely to be a significant deterrent. This seems to be the experience in the United States, where there have been more and larger claims,[155] and there is little reason to think the situation would be better in Canada.

Even on the most optimistic view, if current trends continue it seems likely that some meritorious claims will go uncompensated and civil litigation will be a fairly weak mechanism for accountability. Not surprisingly, then, a number of scholars have called for the creation of additional provisions for damages or statutory rights of action.[156] This would have a limited effect on the patchwork problem, since apart from federal legislation enhancing the availability of damages under *PIPEDA* or creating an equivalent public sector provision, initiatives across the country could further exacerbate differences. Legislation could, however, address some of the limitations of common law actions. Strengthening other forms of accountability and oversight is another obvious possibility and should not be neglected even if civil claims are viable. In the absence of legislative reform, the progressive development of the law on some of the issues identified here could help to clarify and expand the options available to address ongoing threats to privacy.

155 Cohen, *supra* note 3 at 536, 569.

156 Chandler, *supra* note 73 at 230, 233; Krueger, *supra* note 102 at 157–59.