ARTICLE

PUBLIC SECTOR PRIVACY BREACHES: SHOULD BRITISH COLUMBIANS HAVE A CAUSE OF ACTION FOR DAMAGES UNDER THE *FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT*?

Naomi J. Krueger

CITED: (2018) 23 *Appeal* 149

INTRODUCTION

The provincial government ("Province") is obligated to protect the personal information it collects from British Columbians, though sometimes it fails to fulfill that obligation. Recent failures include privacy breaches at the Ministry of Health and Ministry of Education. In June 2013, there were three unauthorized data disclosures at the Ministry of Health. Following those breaches Elizabeth Denham, then the Information and Privacy Commissioner for British Columbia ("Commissioner"), released an investigation report highlighting significant deficiencies in the Ministry of Health's privacy and security safeguards for personal information.[1] In September 2015, the Ministry of Education reported the loss of an unencrypted hard drive containing the personal information of millions of students and teachers from British Columbia and Yukon.[2] After investigating the loss, the Commissioner determined that several Ministry of Education employees had violated the privacy and security safeguards aimed at preventing the unauthorized use, access, and disclosure of private records.[3] Through those failures, the Province exposed millions of British Columbians (and Yukoners) to risk, including the risks of identity theft and loss of reputation—and the mental distress and economic losses that can accompany those risks.

In this paper, I argue that the Province's obligation to make reasonable security arrangements against unauthorized access, collection, use, and disclosure of personal information

1 British Columbia, Office of the Information and Privacy Commissioner, *Investigation Report F13-02*: *Ministry of Health*, 2013 BCIPC No 14 [*Investigation Report: Ministry of Health*]. The Office of the Information and Privacy Commissioner for British Columbia was established in 1993 to oversee and enforce British Columbia's privacy laws. The Commissioner is tasked with, among other things, investigating reported privacy breaches. After investigating a privacy breach, the Commissioner may choose to publish an investigation report setting out any findings of law or recommendations for remedying a breach or complaint or to prevent future breaches: for more about the OIPC, see Office of the Information and Privacy Commissioner, "Home", online: <www.oipc.bc.ca> archived at <https://perma.cc/YF9X-3W9E>.

2 Office of the Information and Privacy Commissioner, News Release, "Statement from BC Information and Privacy Commissioner regarding a Ministry of Education Privacy breach" (22 September 2015).

3 British Columbia, Office of the Information and Privacy Commissioner, *Investigation Report F16-01: Ministry of Education,* 2016 BCIPC No 5 at 4 [*Investigation Report: Ministry of Education*].

pursuant to the *Freedom of Information and Protection of Privacy Act* ("*FIPPA*")[4] is of limited value to British Columbians as the statute prohibits actions against the Province for good faith disclosures. In particular, I suggest that British Columbians should have access to a cause of action in damages to recover losses arising from privacy breaches by the Province.[5]

In Part I of this paper, I look at the scope of the Province's obligation to protect the personal information of British Columbians. Then, to illustrate the lack of remedies available under *FIPPA*, I compare its provisions with the cause of action for damages under the *Personal Information Protection Act* ("*PIPA*").[6] I then consider the Commissioner's findings as to the nature of the breaches at the Ministry of Health and Ministry of Education and her findings about the manner in which the breaches occurred.

I also consider whether the *Privacy Act* would provide a cause of action against the Province for British Columbians harmed by the unauthorized disclosures in those circumstances,[7] though I conclude that because the *Privacy Act* only gives rise to damages for intentional conduct, the Province would likely not be liable for the privacy breaches in the absence of evidence they were intentional (within the meaning of the *Privacy Act*).

In Part II, I argue *FIPPA* should be amended to include a cause of action for damages, even if only to provide access to nominal damages for British Columbians harmed by privacy breaches. Such an amendment is necessary to recognize the scope of risk British Columbians take when they provide personal information to the Province. To illustrate the risk taken, I give an overview of the type of damages claimed in private law cases where privacy breaches similar to those at the Ministry of Health and Ministry of Education have occurred. While some Courts have maintained that emotional distress is more than an inconvenience in certain circumstances, others have applied *Mustapha v Culligan of Canada Ltd*[8] to narrow the scope of compensable losses for breach of privacy. Accordingly, I argue that unauthorized access and disclosure under *FIPPA* should be actionable *per se* to allow plaintiffs to recover nominal damages.

Lastly, in Part III, I argue British Columbians should be able to seek damages in negligence from the Province when they suffer actual harm because of the Province's negligent protection of personal information. I rely on the Commissioner's findings with respect to the Ministry of Health and Ministry of Education breaches to argue that the Province breached a private law duty of care owed to British Columbians when it failed to supervise and enforce the protection of personal information at those Ministries.

---

4 *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165 [*FIPPA*].

5 In this paper, I focus exclusively on whether British Columbians should be able to claim damages from the Province for what I argue is negligent conduct in relation to personal information. I do not address any possible claims for breach of contract or breach of fiduciary duty.

6 *Personal Information Protection Act*, SBC 2003, c 63 [*PIPA*]. Among other things, *PIPA* regulates the collection and use of personal information in the private sector.

7 *Privacy Act*, RSBC 1996, c 373 [*Privacy Act*]. My analysis is limited in the sense that it is based solely on the facts available in the investigation reports; however, the Commissioner's findings would likely be persuasive in the context of litigation given her authority to determine all questions of fact and law pursuant to section 56 of *FIPPA*.

8 *Mustapha v Culligan of Canada Ltd*, 2008 SCC 27 [*Mustapha*]. In *Mustapha*, the plaintiff claimed damages for a psychiatric injury, which he said was the result of having found a fly in a water bottle delivered to him by the defendant. Chief Justice McLachlin, for the Court, held that the plaintiff's psychiatric injury was not compensable under the negligence analysis because a reasonable person would not have suffered the type of injury he suffered as a result of the alleged breach of the duty of care. In cases where a person's psychiatric injuries do not flow from a physical injury, the alleged injury must be a reasonably foreseeable result of the conduct or negligence at issue.

I. OVERVIEW OF BRITISH COLUMBIA'S PRIVACY LEGISLATION

The Province routinely gathers and stores a significant amount of personal information from British Columbians. The information gathered is generally necessary for policy development and service delivery in British Columbia.[9] The types of information British Columbians entrust to the Province include contact information and addresses, personal health numbers, driver's license numbers, and social insurance numbers. This information may include details about a person's occupation, income, or family structure. In medical circumstances, it may include information about a diagnosis or treatment of an illness.

Recognizing the sensitive nature of this type of information, the Legislative Assembly of British Columbia unanimously passed *FIPPA* in June 1992. When it was enacted, *FIPPA* only applied to provincial public bodies, including government ministries, provincial government corporations, boards, commissions, and agencies.[10] Soon after, *FIPPA* was amended to apply to "local public bodies" including local and regional governments, hospitals, police forces and boards, schools, school boards, universities, colleges, and self-governing professional bodies.[11] The overarching purpose of *FIPPA* is to "provide greater protection for privacy with respect to personal information held by the government," to limit the government's right to collect infomation, and to limit the way it can use the information it collects.[12]

A. Personal information is broadly defined

FIPPA defines personal information as "any recorded information about an identifiable individual other than contact information."[13] The Office of the Information and Privacy Commissioner for British Columbia ("OIPC") has interpreted that definition broadly to include any recorded information that uniquely identifies a person, such as the person's name, address and telephone number (when stored with other identifying information), age, sex, race, religion, sexual orientation, disability, fingerprints, or blood type.[14] Third-party opinions about British Columbians and the opinions of British Columbians about themselves are generally protected under *FIPPA* as well.[15] To be considered "personal information," the information must be reasonably capable of identifying a particular individual either alone or with other sources available to those seeking it, and it must be collected, used, or disclosed for a purpose related to the individual.[16]

---

9 Barbara McIsaac, Rick Shields & Kris Klein, *The Law of Privacy in Canada* (Toronto: Carswell, 2016), 3.31-3.3.3.

10 *Freedom of Information and Protection of Privacy Act*, *1992*, SBC 1992, c 61; McIsaac, Shields & Klein, *supra* note 9, s 3.3.1.

11 *Freedom of Information and Protection of Privacy Amendment Act, 1993*, SBC 1993, c 46; McIsaac, Shields & Klein, *supra* note 9. Although *FIPPA* applies broadly to public bodies, I refer specifically to the Province throughout this paper because I draw from the Ministry of Health and Ministry of Education breaches to frame my analysis.

12 British Columbia, Legislative Assembly, *Debates of the Legislative Assembly of British Columbia (Hansard)*, 35th Parl, 1st Sess, Vol 3, No 12 (22 May 1992) at 173 (Hon C Gabelmann).

13 *FIPPA, supra* note 4, schedule 1.

14 British Columbia, Office of the Information and Privacy Commissioner, "Guide to Access and Privacy Protection under *FIPPA*" (October 2015) at 4 ["Guide to *FIPPA*"].

15 *Ibid*. See also *Harrison v British Columbia (Information and Privacy Commissioner)*, 2008 BCSC 411 at para 42 where the Court held that a Ministry of Child and Family Development resource worker's opinion about the level of risk Robert Glen Harrison posed to children and youth was protected by legislation as personal information.

16 McIsaac, Shields & Klein, *supra* note 9.

B. *FIPPA* imposes privacy protection obligations on the Province

One of *FIPPA*'s primary purposes is to create accountability for public bodies that collect personal information from British Columbians and the greater public.[17] *FIPPA* regulates how public bodies collect, use, and disclose personal information and ensures that personal information is handled fairly.[18] *FIPPA* recognizes the inherent right of British Columbians to retain some control over information disclosed in exchange for services.[19] In essence, *FIPPA* attempts to balance that right with the need to collect personal information in the course of providing services to British Columbians.

Under section 30 of *FIPPA*, the Province is required to protect personal information in its custody or under its control by making reasonable security arrangements against risks such as unauthorized access, collection, use, disclosure, or disposal.[20] The Commissioner has held that reasonable security arrangements are measured on an objective basis, and while perfection is not required, the type of information gathered determines the level of protection that is necessary.[21] In the investigation report on the Ministry of Health disclosures, the Commissioner said:

> To meet the reasonableness standard for security arrangements, public bodies must ensure that they have appropriate administrative, physical and technical safeguards. The measure of adequacy for these safeguards varies depending on the sensitivity of the personal information, the medium and format of the records, the estimated costs of security, the relationship between the public body and the affected individuals and how valuable the information might be for someone intending to misuse it.[22]

Additionally, *FIPPA* prohibits the Province from disclosing personal information except in accordance with the legislation, and it requires the Province to report any unauthorized disclosures immediately upon discovery of the disclosure.[23] Unauthorized disclosures are punishable offenses and subject to a fine of up to CAD2,000 for individuals and CAD500,000 for corporations.[24]

The OIPC is responsible for monitoring the Province's compliance with its *FIPPA* obligations.[25] Sections 42(2) and 44 of *FIPPA* set out the broad powers of the Commissioner to investigate and resolve any complaints from the public, including complaints about unperformed duties or personal information that has been improperly collected, used, or disclosed by the Province.[26] The Commissioner has jurisdiction to decide all questions of

---

17 *FIPPA, supra* note 4, s 2. *FIPPA* also contains provisions that regulate when and how the public will be permitted to access government records.

18 *FIPPA, supra* note 4.

19 McIsaac, Shields & Klein, *supra* note 9.

20 *FIPPA, supra* note 4, s 30.

21 *Investigation Report: Ministry of Health*, *supra* note 1 at 9; *Investigation Report: Ministry of Education*, *supra* note 3 at 11.

22 *Investigation Report: Ministry of Health*, *supra* note 1. For more on how to manage personal information, see Michael Power, "Annex: Managing Personal Information" in *The Law of Privacy* (Markham: LexisNexis Canada Ltd, 2013) at 265.

23 *FIPPA, supra* note 4 at ss 30.4 and 30.5. Sections 33.1, 33.2, and 33.3 describe circumstances where authorized disclosures of personal information may be permitted.

24 *Ibid*, ss 30.4, 30.5, and 74.1.

25 *Ibid*, ss 42 and 44.

26 *Ibid*.

fact and law, and can make an order under section 58 to dispose of any compliance issues that arise.[27] The Commissioner may, by order, do one or more of the following:

> 58(3)(a) confirm that a duty imposed under this Act has been performed or require that a duty imposed under this Act be performed;
>
> […]
>
> (e) require a public body or service provider to stop collecting, using or disclosing personal information in contravention of this Act, or confirm a decision of a public body or service provider to collect, use or disclose personal information;
>
> (f) require the head of a public body to destroy personal information collected in contravention of this Act.[28]

Section 74 of *FIPPA* makes it an offence to not comply with an order issued by the Commissioner; but the Commissioner has no jurisdiction to make an order for damages in circumstances where a breach has caused harm.[29] Instead, the Province is protected by section 73 of *FIPPA*, which bars any and all claims for "good faith" disclosures, meaning that absent evidence of bad faith, the Province is immune from liability for harm or loss flowing from a privacy breach.[30]

C. The *Personal Information Protection Act* governs the private sector

PIPA, which came into force on January 1, 2004, similarly governs the collection, use, and disclosure of personal information—but in the private sector.[31] When *PIPA* was introduced in the Legislative Assembly of British Columbia on April 30, 2003, it was said to reflect the Province's commitment to ensuring that private sector businesses in British Columbia were well positioned to take full advantage of commercial opportunities, especially in electronic commerce, while also reassuring British Columbians that their personal information is protected when they participate in electronic transactions.[32] *PIPA*'s purpose mirrors that of *FIPPA* in that it aims to balance the right of individuals to protect their personal information and the need of organizations to collect, use, and disclose information in the normal course of business.[33]

Unlike *FIPPA, PIPA* provides a statutory cause of action for damages, which permits British Columbians to recover damages for privacy breaches that occur as a result of a private sector organization's failure to adhere to the obligations set out in that legislation.[34]

In British Columbia's private sector, organizations cannot collect, use, or disclose personal information without the consent of the relevant individual, and even then, they can only use collected information for "reasonable purposes."[35] What is reasonable will depend on a

---

27 *Ibid*, s 56.

28 *Ibid*, s 58.

29 *Ibid*, s 74. Whether the Commissioner should be authorized to award damages for public sector breaches is not discussed to any significant length in this paper; however, such a power may be sufficient to enable British Columbians to recover damages up to a certain amount.

30 *Ibid*, s 73. I explore the operational effect of this provision in Part II, below.

31 McIsaac, Shields & Klein, *supra* note 9, s 4.3.1; *PIPA, supra* note 6.

32 British Columbia, Legislative Assembly, *Debates of the Legislative Assembly of British Columbia (Hansard)*, 37th Parl, 4th Sess, Vol 14 No 12 (30 April 2003) at 1419 (Hon S Santoni).

33 *PIPA, supra* note 6, s. 2; McIsaac, Shields & Klein, *supra* note 9, s 4.3.2; British Columbia, Office of the Information and Privacy Commissioner, Order P05-01 (May 25, 2005) at paras 38-43 and 55.

34 McIsaac, Shields & Klein, *supra* note 9; *PIPA, supra* note 6, s 57. See also *FIPPA*, *supra* note 4, s 73.

35 *PIPA, supra* note 6, ss 6, 11, 14, 17 and 26.

range of factors, including the kind or amount of personal information collected, how the information is going to be used, and where and how the information will be disclosed.[36] An organization must develop and follow the policies and practices necessary to meet its obligation to protect the personal information it chooses to collect.[37]

As with public sector privacy breaches, the Commissioner has broad powers to investigate complaints about private sector privacy breaches. After an investigation, however, the Commissioner is required to make a binding order that disposes of the issues of the investigation.[38]

After the Commissioner makes an order, section 57 of *PIPA* creates a cause of action for damages:

> 57(1) If the commissioner has made an order under this Act against an organization and the order has become final as a result of there being no further right of appeal, *an individual affected by the order has a cause of action against the organization for damages for actual harm that the individual has suffered as a result of the breach by the organization of obligations* under this Act.
>
> (2) If an organization has been convicted of an offence under this Act and the conviction has become final as a result of there being no further right of appeal, *a person affected by the conduct that gave rise to the offence has a cause of action against the organization convicted of the offence for damages for actual harm that the person has suffered as a result of the conduct*.[39]

By permitting an action for damages, this section provides a meaningful remedy to British Columbians whose privacy has been breached by a private sector organization.[40]

D. The *Privacy Act* grants a limited private right of action in British Columbia

If an individual in British Columbia suffered a harm or loss because of the Ministry of Health or Ministry of Education privacy breaches, it is unlikely that a claim for damages would arise pursuant to the *Privacy Act*. Currently, absent a finding of bad faith, British Columbians can only recover damages from the Province for an unauthorized disclosure of personal information under the vicarious liability doctrine and pursuant to the *Privacy Act*.

The *Privacy Act* provides that "it is a tort, actionable without proof of damage, for a person, willfully and without a claim of right, to violate the privacy of another."[41] The Commissioner's investigation reports indicate that both the Ministry of Health and

---

36 "Guide to *FIPPA*", *supra* note 14.

37 *PIPA, supra* note 6, s 4(1), and ss 11, 14 and 17; see also McIsaac, Shields & Klein, *supra* note 9.

38 *PIPA, supra* note 6, ss 50 and 52. If, for example, after investigating a complaint about a privacy breach under *PIPA*, the Commissioner finds that an organization has not adequately performed the duties set out in the act, she can make an order requiring the organization to perform those duties. Conversely, if the Commissioner finds that the organization has adequately performed the duties under the act, she can make an order to that effect. Either way, she must make an order that resolves the issues giving rise to the investigation.

39 *Ibid*, s 57 [emphasis added].

40 A right is only as meaningful as the remedy provided for its breach: *R v 974649 Ontario Inc*, 2001 SCC 81 at para 20. A discussion of whether *PIPA* should provide a cause of action for damages without proof of "actual harm" is beyond the scope of this paper; however, a provision similar to section 57 in *FIPPA* may be all that is needed to recognize the impact that similar public sector privacy breaches can have on British Columbians.

41 *Privacy Act*, *supra* note 7, s 1. See for example *Ari v Insurance Corporation of British Columbia,* 2013 BCSC 1308 [*Ari* BCSC], aff'd *Ari v Insurance Corporation of British Columbia,* 2015 BCCA 468 at paras 51-61 [*Ari* BCCA]; *Albayate v Bank of Montreal*, 2015 BCSC 695 [*Albayate*].

Ministry of Education breaches were caused by the Province's carelessness rather than a single employee or group of employees intentionally harmful conduct.[42] If the Commissioner had found the privacy breaches were intentionally caused by employees at either of those Ministries, the Province might face liability under the doctrine of vicarious liability.[43] British Columbians claiming damages against the Province in those circumstances would need to show that an employee or a group of employees of the Ministry of Health or Ministry of Education willfully and without a claim of right violated their privacy—and that those violations arose in the course and scope of employment—before the Courts would apply the doctrine of vicarious liability to award damages, payable by the Province, for the conduct of an employee or group of employees.

As I set out in greater detail below, the Commissioner found that the Ministry of Health and Ministry of Education privacy breaches were caused by the Province's carelessness, rather than the intentionally injurious conduct of an employee or group of employees. It is, therefore, unlikely that British Columbians could claim for damages under the *Privacy Act* and the vicarious liability doctrine.

i. The Ministry of Health Disclosures

In May 2012, the Ministry of Health reported three unauthorized disclosures of personal health information at its Pharmaceutical Services Division.[44] On those three separate occasions, Ministry of Health employees transferred personal information about British Columbians to portable storage devices and gave the information to researchers employed (or contracted) by the Province.[45] The disclosures did not include names of health care recipients, but they did include Personal Health Numbers and other demographic information that could be used to identify individuals and their sensitive health information.[46] One of the disclosures included information about the alcohol and drug use, mental health, self-esteem, and sexual health of some British Columbians. The Ministry of Health admitted that the disclosures were unauthorized under *FIPPA*.[47]

The Commissioner investigated the disclosures and found that they each occurred because of deficiencies in the Ministry of Health's privacy and security safeguards for personal information.[48] She found specifically that the Ministry of Health lacked effective governance, management, and controls over access to personal health information, deficiencies that were exacerbated by a lack of clear responsibility for privacy and security.[49] Most notably, employees were able to copy large quantities of personal health data onto unencrypted flash drives and share the data with unauthorized persons without being detected by the Ministry of Health's privacy or security controls, in place to prevent such disclosures.[50] The Commissioner found that Ministry of Health employees had excessive access to personal information.[51] At the same time, there was a complete lack of monitoring, enforcement, or evaluation of unauthorized access, use, and disclosure of personal information. There were

---

42 *Investigation Report: Ministry of Health*, *supra* note 1.

43 *Ari* BCSC, *supra* note 41; *Ari* BCCA, *supra* note 41. Under the doctrine of vicarious liability, an employer can be held liable for an employee's tortious conduct or omission if the employee's conduct or omission arises in the course and scope of his or her employment. The doctrine of vicarious liability provides an exception to the general proposition that liability for tortious conduct or omissions will lie exclusively with the tortfeasor.

44 *Investigation Report: Ministry of Health*, *supra* note 1 at 5.

45 *Ibid*.

46 *Ibid*.

47 *Ibid* at 10.

48 *Ibid* at 3.

49 *Ibid* at 5.

50 *Ibid* at 5 and 12.

51 *Ibid* at 14.

absolutely no audits of employee or researcher compliance with the privacy provisions in the agreements that authorized information sharing.[52] Although the Ministry of Health had privacy and security policies in place, the Commissioner found that it had failed to translate those policies into meaningful business practices.[53]

ii. The Ministry of Education Disclosures

The Province reported a similar breach to the OIPC on September 18, 2015 after it learned that the Ministry of Education was unable to locate an unencrypted portable hard drive containing the personal information of about 3.4 million British Columbian and Yukoner students and teachers.[54] The missing information included names, genders, birthdates, addresses, and other identifying details collected over a period of more than 10 years.[55] The hard drive was last seen in May 2011, in a locked cage, at an offsite warehouse leased by the Ministry of Education.[56]

When the Commissioner investigated the breach, she learned that a team of Ministry of Education employees had been analyzing education data to produce reports related to student performance and the overall performance of the education system.[57] After the reports were complete, the analysts transferred their project files on to two mobile hard drives to decrease electronic storage costs.[58] One hard drive was used by the employees for follow up questions and reports, and the other was created as a backup and was taken to an offsite warehouse for storage.[59] The Ministry of Education discovered the backup hard drive was missing in July 2015 when an employee went to the warehouse to retrieve it.[60]

Again, the Commissioner found that though the Province had adequate policies in place to protect personal information, it had failed to properly enforce those policies at the Ministry of Education.[61] The employees who transferred the unencrypted data to the hard drives were aware of the privacy and security policies in place, and they were aware that transferring the data was a clear violation of at least three of those policies.[62] First, the employees failed to encrypt the information; second, they failed to properly record the existence of the hard drives in an inventory of information assets; and finally, they failed to store the backup hard drive in a government approved records facility.[63] The Commissioner was of the view that the training received by staff and managers was not effective in ensuring compliance with the policies in place to protect personal information at the Ministry of Education.[64]

Although the Commissioner's findings highlight the Province's failure to follow the policies it put in place to protect the personal information of British Columbians, there is insufficient information to conclude that any one employee accessed, used, or disclosed that information in bad faith. Rather, the reports suggest that the various systemic failures within the two Ministries, including the Province's failure to monitor the authorized

---

52 *Ibid* at 15.
53 *Ibid* at 3.
54 *Investigation Report: Ministry of Education*, *supra* note 3 at 4.
55 *Ibid* at 6.
56 *Ibid*.
57 *Ibid* at 8.
58 *Ibid* at 10.
59 *Ibid*.
60 *Ibid*.
61 *Ibid* at 20.
62 *Ibid*.
63 *Ibid* at 15.
64 *Ibid*.

conduct of employees were operational in nature. In the absence of a clearly intentional breach of privacy, the *Privacy Act* would not offer a right of action to British Columbians harmed by either one of the breaches.

II. NOMINAL DAMAGES FOR PUBLIC SECTOR PRIVACY BREACHES

Without an action for damages, the Province's obligation to make reasonable security arrangements to protect personal information is of limited value to British Columbians when measured against the risks they take entrusting their personal information to the Province. To fairly reflect the scope of that risk, *FIPPA* should be amended to include a cause of action for damages, even in the absence of bad faith.

Currently, section 73 bars any and all claims against the Province for "good faith" disclosures.[65] It grants near-immunity to the Province by providing that:

> 73 No action lies and no proceeding may be brought against the government, a public body, the head of a public body, an elected official of a public body or any person acting on behalf of or under the direction of the head of a public body for damages resulting from
>
> (a) the disclosure, or failure to disclose, in good faith of all or part of a record under this Act or any consequences of that disclosure or failure to disclose, or
>
> (b) the failure to give any notice required under this Act if reasonable care is taken to give the required notice.[66]

While it is open to the legislature to limit the Province's liability in circumstances it deems appropriate, *FIPPA*'s purpose is to create accountability for public bodies that collect personal information from British Columbians. In light of that purpose, an immunity clause is difficult to reconcile with the reality that British Columbians often have no choice but to provide the Province with their personal information in order to receive services such as health care and educational programming.[67]

A. The harms associated with unauthorized disclosures are generally psychological in nature

In *Condon v Canada,* Justice Gagné certified a class action against Canada's Ministry of Human Resources and Skills Development after it lost an external hard drive with the personal information of approximately 583,000 Canadians, including the names, dates of birth, addresses, student loan balances, and social insurance numbers of those individuals.[68] In their motion to certify, the plaintiffs acknowledged that their claims for damages were "for very small sums."[69] They sought compensation for "wasted-time, inconvenience, frustration and anxiety" resulting from the lost hard drive and damages for "increased risk of identity theft in the future."[70] Other plaintiffs have claimed damages for the same or similar injuries, including "anxiety, inconvenience, pain, suffering and/or fear due to

65 *FIPPA, supra* note 4, s 73.

66 *Ibid.*

67 British Columbia, Office of the Information and Privacy Commissioner, "An Examination of British Columbia's Privacy Breach Management" (28 January 2015) at 3 ["Privacy Breach Management"].

68 *Condon v Canada*, 2014 FC 250 at paras 2, 117 [*Condon*], aff'd *Condon v Canada,* 2015 FCA 159.

69 *Condon, supra* note 68 at para 49.

70 *Ibid* at para 66.

the loss of their personal information" and for exposure to fraud and/or identity theft.[71] More specifically, plaintiffs have alleged that, even in the absence of actual economic loss or other consequences of identity theft, "fear, stress, inconvenience and loss of time due to the necessity of monitoring monthly statements of accounts" are compensable injuries.[72]

Despite the seriousness of the injuries alleged, Courts have consistently relied on *Mustapha,* where the Supreme Court of Canada ("SCC") drew a distinction between minor and transient upsets and compensable injuries, to restrict the circumstances where damages for breach of privacy will be awarded.[73] Generally, harms associated with privacy breaches are considered to be "ordinary annoyances, anxieties, and fears that people living in society routinely, if sometimes reluctantly, accept," so actual harm seems to be a difficult threshold to cross.[74]

B. Nominal damages are an appropriate remedy in the circumstances

In British Columbia, nominal damages may be available to a plaintiff who cannot meet the threshold of actual harm following a privacy breach. Nominal damages are defined as "a trivial sum of money awarded to a litigant who has established a cause of action but has not established entitlement to compensatory damages."[75] The purpose of nominal damages is to establish individual rights and to recognize a defendant's liability when those rights have been violated in an unacceptable way.[76] Given the costs associated with litigation of this nature, it may not be cost effective for an individual British Columbian to bring an action against the Province for nominal damages alone; however, class proceedings may permit British Columbians to have their privacy rights recognized when they have been violated by the Province.[77] As set out above, in privacy breach cases, the Courts have awarded nominal damages to recognize psychological harms associated with privacy breaches.

In *Nammo v TransUnion of Canada Inc* ("*Nammo*"), the Federal Court awarded Mirza Nammo CAD5,000 to recognize the humiliation he suffered after the Royal Bank of Canada denied him a business loan because the defendant, TransUnion, provided the bank with credit information that was incorrect.[78] Nammo sought damages under section 16 of the *Personal Information Protection and Electronic Documents Act* ("*PIPEDA"*), which provides that "[t]he Court may, in addition to any other remedies it may give […] award damages to the complainant, including damages for any humiliation that the complainant has suffered."[79]

---

71 *Mazzonna c DaimlerChrysler Financial Services Canada Inc/Services financiers DaimlerChrysler inc*, 2012 QCCS 958 at para 10 [*Mazzonna*].

72 *Ibid*; *Zuckerman c Target Corporation*, 2015 QCCS 1285 at para 12 [*Zuckerman*]; *Larose c Banque Nationale du Canada*, 2010 QCCS 5385.

73 *Mazzonna, supra* note 71*; Zuckerman, supra* note 72.

74 *Mustapha, supra* note 8 at para 9.

75 Ken Cooper-Stephenson, *Personal Injury Damages in Canada* (Toronto: Carswell, 1996) at 99.

76 *Ibid* at 100, 101.

77 See for example *Tucci v Peoples Trust Company*, 2017 BCSC 1525 [*Tucci*]. In *Tucci*, the British Columbia Supreme Court ("BCSC") certified, as a class proceeding, an action against the defendant by representative plaintiffs who may be at risk of identity theft because an online database containing personal information they provided to the defendant had been accessed by unauthorized individuals located in another country. The representative plaintiffs claimed, among other things, a nominal award to recognize time wasted, inconvenience, frustration, anger, or stress flowing from the breach of their privacy.

78 *Nammo v TransUnion of Canada Inc*, 2010 FC 1284 at para 7 [*Nammo*].

79 *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 [*PIPEDA*]; *ibid* at paras 66 and 75. *PIPEDA* governs private sector organizations in provinces without similar legislation, and it governs all private organizations that engage in interprovincial or international commercial transactions. For more about the significance of *PIPEDA* in Canada, see *Eastmond v Canadian Pacific Railway*, 2004 FC 852.

Notably, *PIPEDA*'s purpose is similar to those of *PIPA* and *FIPPA. PIPEDA*'s purpose is set out in section 3, which reads:

> 3 The purpose of this Part [Protection of Personal Information in the Private Sector] is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.[80]

In *Nammo,* the Federal Court said that disseminating false credit information lays a person bare to those receiving the information: "having wrong information shared about you can be equally intrusive, embarrassing and humiliating as a brief and respectful strip search."[81] Although the effects of humiliation are difficult to prove, *Nammo* recognizes that in some circumstances, they are much more than ordinary annoyances, anxieties and fears that people should generally be able to cope with in society.

Applying *Nammo*, the BCSC awarded CAD2,000 in nominal damages in *Albayate v Bank of Montreal,* to recognize the banking inconveniences suffered by Loretta Albayate after her bank provided two credit bureaus with inaccurate information about her address.[82] Albayate claimed damages under the *Privacy Act* but did not succeed in establishing that she suffered actual psychological harm because of the privacy breach.[83] To recover damages for emotional or psychological harm under the *Privacy Act* there must be actual damage, meaning the psychological harm must rise to the level of a recognizable psychiatric illness.[84] Nevertheless, the BCSC recognized that her right to privacy had been violated in a manner that warranted an award of nominal damages.[85]

The scope of damages claimed in these cases illustrates the potential consequences of the Ministry of Health and Ministry of Education privacy breaches for individuals whose information has been accessed or disclosed without authorization. Even if only in the context of a class proceeding, nominal damages under *FIPPA* would provide a meaningful remedy for British Columbians because such a claim would permit recovery of modest losses and would have the effect of enforcing privacy rights against the Province.

III. NEGLIGENCE LAW OFFERS IMPORTANT REMEDIES AND ENFORCEMENT OPTIONS TO BRITISH COLUMBIANS

Without a statutory cause of action for damages, British Columbians should be able to rely on the law of negligence to enforce their privacy rights against the Province. When the *Crown Proceedings Act* was enacted,[86] the law of negligence became an important vehicle for British Columbians to voice their complaints and to secure remedies for the Province's carelessness.[87] In the investigation reports, the Commissioner was clear that the Ministry of Health and Ministry of Education breaches occurred because the Province failed to

---

80 *PIPEDA, supra* note 78, s 3; see also McIsaac, Shields & Klein, *supra* note 9.

81 *Nammo*, *supra* note 78 at para 78.

82 *Albayate, supra* note 41.

83 *Ibid* at paras 138, 144.

84 *Kotai v The Queen of the North (Ship)*, 2009 BCSC 1405 at para 69, applied in *Albayate, supra* note 41. However, see *Saadati v Moorhead*, 2017 SCC 28 for a recent consideration of the proof required for psychiatric injuries.

85 *Albayate, supra* note 41.

86 *Crown Proceedings Act*, SBC 1974, c 24.

87 Phillip H Osbourne, *The Law of Torts* (Toronto: Irwin Law, 2015) at 224-225.

supervise and enforce the privacy protection obligations imposed under *FIPPA*. If British Columbians suffer actual harm as a result of the Province's carelessness, they should be able to recover their losses in negligence.

A. The Courts addressed negligence in *Ari v Insurance Corporation of British Columbia* ("*Ari*")

In November 2015, the British Columbia Court of Appeal ("BCCA") held that section 30 of *FIPPA* does not give rise to a private law duty of care to make reasonable arrangements to protect against unauthorized access, collection, use, disclosure, or disposal of personal information.[88] *Ari* was proposed as a class action against the Insurance Corporation of British Columbia ("ICBC") after an ICBC employee accessed the personal information of Ufuk Ari and 65 other ICBC clients without an apparent business purpose.[89] In chambers, Justice Russell allowed Ari's claim for vicarious liability under the *Privacy Act,* but struck his claims for common law breach of privacy and for negligent protection of private information.[90] On appeal, the BCCA affirmed that there is no common law tort of breach of privacy in British Columbia. It also reiterated the rule in *R v Saskatchewan Wheat Pool*[91] that protects public bodies from liability in negligence for merely breaching a statutory duty.[92]

On the question of whether a new private law duty of care could require ICBC to make reasonable arrangements to protect personal information, the Court found that notwithstanding foreseeability of harm and proximity, four policy considerations negated such a duty.[93] First, the Court found that recognizing a duty of care would raise the specter of indeterminate liability because of *FIPPA*'s broad application to all public bodies.[94] Second, it recognized that because *FIPPA* does not legislate a specific standard of care, a range of acceptable conduct is permitted by that legislation; any security arrangements implemented would understandably vary depending on the nature of the public body.[95] Third, the Court held that Ari's claim was related specifically to the reasonableness of ICBC's security measures, not the actual manner or extent to which the measures were carried out by ICBC and its employees.[96] Finally, after reviewing the comprehensive complaint and remedy scheme under *FIPPA*, the Court held that the legislature had no intention of allowing a common law remedy to exist alongside the remedies available in the statute.[97]

B. *Ari* is distinguishable on the facts

FIPPA, without section 73, would likely give rise to a private law duty of care for British Columbians who suffered loss as a result of the Ministry of Health and Ministry of Education breaches because *Ari* can be distinguished in two critical ways on the facts available. First, based on the Commissioner's investigation reports, any claims against the Province would stem from its failure to supervise and enforce the operational aspects of protecting the personal information of British Columbians. In *Ari,* Justice Russell rejected

---

88 *Ari* BCCA, *supra* note 41 at para 53..

89 *Ari* BCSC, *supra* note 41 at para 3.

90 *Ibid* at paras 65, 79.

91 *R v Saskatchewan Wheat Pool,* [1983] 1 SCR 205 [*"Saskatchewan Wheat Pool"*].

92 *Ari* BCCA, *supra* note 41 at paras 19, 20. See also *Holland v Saskatchewan,* 2008 SCC 42; *Saskatchewan Wheat Pool, supra* note 91 at 225. In *Saskatchewan Wheat Pool,* the SCC held that statutory breaches will be considered in the context of the general law of negligence. Statutory breach is not a tort in and of itself.

93 *Ari* BCCA, *supra* note 41 at para 48.

94 *Ibid* at para 50.

95 *Ibid* at para 51.

96 *Ibid* at para 52.

97 *Ibid* at paras 53-62.

the argument that Ari's claim was analogous to *KLB v British Columbia* ("*KLB*") insofar as it involved liability for breach of a statutory duty, because *KLB* "dealt with negligence arising out of the operational acts of government."[98]

In *KLB*,[99] the SCC held that the Province had a duty under the *Protection of Children Act* to "place children in adequate foster homes and to supervise their stay" in those homes.[100] At the time, the *Protection of Children Act* required the Superintendent of Child Welfare to make arrangements for the placement of a child in a foster home "as will best meet the needs of the child."[101] The SCC recognized that the Province could not be a "guarantor against all harm" but it held that the Province would be responsible for harm sustained by children if the Province failed to adequately monitor and respond to any abuse detected in foster homes.[102] Similarly, British Columbians should be able to expect that the Province will monitor its employees to ensure that the personal information it collects is being adequately protected under *FIPPA* and that it will respond to any detected access or unauthorized disclosure.

Second, while the core duty of care would flow from section 30 of *FIPPA*, other provisions are fundamentally relevant. For example, sections 26(d)(i) and 27(2) require the individual subject of the information to give informed consent to its collection, section 30.4 prohibits unauthorized disclosures, and section 32 limits the way personal information can be used by the public body who collected the information. Each of these provisions may inform whether a proximate relationship can be established between the Province and British Columbians. If an individual has been assured by the Province that the information it is collecting will be used only for a particular purpose and will not be disclosed without authorization, the Province should be expected to adequately supervise and enforce the policies and mechanisms put in place to meet expectations of privacy established by those assurances.[103]

C. In the circumstances, *FIPPA* gives rise to a *prima facie* duty of care

I argue that *FIPPA*'s privacy protection provisions give rise to at least two different duties of care.

First, the Ministry of Health and Ministry of Education breaches may give rise to a claim for negligent misrepresentation. In *R v Imperial Tobacco Canada Ltd,* the SCC stated that:

> a special relationship will be established where (1) the defendant ought reasonably to foresee that the plaintiff will rely on his or her representation; and (2) reliance by the plaintiff would be reasonable in the circumstances of the case […] Where such a relationship is established, the defendant may be liable for losses suffered by the plaintiff as a result of a negligent misstatement.[104]

General statements by the Province to the public about privacy mechanisms implemented under *FIPPA* are not sufficient to establish a proximate relationship. However, if the Province, in an authorization form, or otherwise, made representations about the

98 *Ibid* at para 20.

99 *KLB v British Columbia,* 2003 SCC 51 [*KLB*].

100 *Ibid* at para 12.

101 *Ibid* at para 13.

102 *Ibid* at para 14.

103 See for example, *Tucci, supra* note 77 at para 131, where the BCSC held that, in the private sector, a duty of care may arise from an organization's own privacy policies and security measures rather than from a legislated standard applicable to public authorities.

104 *R v Imperial Tobacco Canada Ltd*, 2011 SCC 42 at para 42 [citations omitted].

mechanisms in place to protect that person's information it should be liable in negligence in circumstances where an individual relied on those statements. If, for example, health care providers or school administrators employed by the Province, in their interactions with a specific individual, led that individual to believe there were adequate safeguards in place to prevent the types of breaches that occurred, the Province and that individual are in a sufficiently proximate relationship to justify a *prima facie* duty of care.

Second, as I have argued throughout, the Province should be liable for negligently supervising and enforcing the arrangements it makes to protect the personal information of British Columbians. The Commissioner's findings clearly indicate the Province had policies in place at both the Ministry of Health and Ministry of Education to govern the conduct of its employees and to protect the personal information of British Columbians. But merely having policies in place is not enough. It is entirely foreseeable that a systemic lack of effective training about policies, monitoring, enforcement, or evaluation of unauthorized access, use, and disclosure of information would expose British Columbians to a significant risk of harm. The law generally accepts that government actors may attract liability in tort if they are negligent in carrying out prescribed duties.[105] Unless a more robust evidentiary record reveals the Province's decisions with respect to supervising and enforcing its duty to protect personal information were made for economic, social, or political reasons, it is reasonable and just to impose a *prima facie* duty of care in the circumstances.

D. Overcoming the policy rationales discussed in *Ari* is difficult but not impossible

Once a *prima facie* duty of care is established, policy reasons for negating a duty of care in the circumstances would have to be considered.[106] In *Ari,* ICBC first argued that recognizing a duty of care would create indeterminate liability because of *FIPPA*'s broad application to all public bodies; the Court agreed.[107] Although indeterminate liability is relevant to the Ministry of Health and Ministry of Education breaches, it is not fatal to either set of circumstances.

In *Hercules Management Ltd v Ernst & Young*, the SCC explained that the prospect of limitless liability checks the imposition of a private law duty of care.[108] The problem of indeterminate liability can be circumscribed by the facts of the Ministry of Health and Ministry of Education breaches. British Columbians seeking damages for negligent misrepresentation would have to establish that their relationship with the Province goes beyond the duty set out in section 30 of *FIPPA*. Only those individuals who can point to an interaction, written or in person, with an employee of the Province who, for the purpose of obtaining consent to collect, use, or disclose personal information, made representations about the Province's privacy protection practices, will be able to recover damages in negligence. Similarly, the Province's liability for negligently supervising and enforcing the operational aspects of privacy protection are constrained by the unique policies of each provincial ministry, agency, board, commission, and Crown corporation. Although, the Province could be liable to a significant number of British Columbians, as described above in Part II, the high threshold for psychological harm set out in *Mustapha*, would naturally limit the scope of compensable damages.

105 *Ibid* at para 71.

106 Osbourne, *supra* note 87 at 77.

107 *Ari* BCCA, *supra* note 41.

108 *Hercules Management Ltd v Ernst & Young,* [1997] 2 SCR 165 at 41.

Second, ICBC argued in *Ari* that the legislature intended to allow a broad range of acceptable privacy protection measures under *FIPPA*.[109] As discussed above, the operational nature of the proposed duty of care limits the relevance of this policy concern in the context of the Ministry of Health and Ministry of Education breaches because the proposed duties are primarily concerned with the Province's failure to monitor and enforce the arrangements it chose to put in place. Furthermore, the Commissioner has set out minimum standards for "reasonable security arrangements" in the course of her investigations into various breaches, and additional interpretation of those standards falls squarely within the role of the Courts in Canada.[110]

In January 2015, the Commissioner released an audit report that examined the degree to which the government was fulfilling its duty to respond to (and properly manage) its privacy breaches.[111] The report made several recommendations to help public bodies reach a minimum standard to enhance the efficacy of breach management programming and to build trust between British Columbians and the government.[112] Arguably, the January 2015 report and the one that followed in September 2015, established a minimum standard of acceptable practices under *FIPPA* and established recommendations to ensure that thorough precautions will be taken to safeguard the personal information of British Columbians.[113]

Lastly, ICBC argued that the British Columbia legislature had no intention of allowing a common law remedy to exist alongside the administrative remedies available under *FIPPA*.[114] On the facts available in the Commissioner's reports, a claim in negligence against the Province, absent a finding of bad faith, could only be filed if section 73 was repealed. As I have argued above, such an amendment would signal to the Courts that the legislature understands the risk British Columbians take when they entrust the Province with their personal information and it would signal to the Courts that individuals harmed by the Province's negligence are entitled to a meaningful remedy for recovering their losses.

CONCLUSION

As long as British Columbians are left without an action in damages for losses suffered because of the Province's failure to protect personal information, *FIPPA* fails to meet its purpose of creating accountability for public bodies that collect personal information from British Columbians. Although the *Privacy Act* provides a cause of action in circumstances where information is deliberately and unlawfully accessed or disclosed, it does not provide a remedy for British Columbians harmed by systemic failures and clear negligence by the Province.[115] Based on the information available about the Ministry of Health and Ministry of Education privacy breaches, it is unlikely that the *Privacy Act* would offer an adequate remedy to British Columbians harmed by those particular breaches.

In privacy breach cases, the significance of the harm to individuals is often considered trivial because it is primarily psychological in nature. The federal government, and the Federal Court, have recognized under *PIPEDA* that some privacy breaches cause humiliation serious enough to warrant a remedy of damages. *FIPPA* needs to be amended to recognize that British Columbians take an incredible risk of experiencing harm, including wasted-time, inconvenience, frustration, anxiety, and increased risk of identity theft when they provide their information to the Province in exchange for services like health care and

109 *Ari* BCCA, *supra* note 41.
110 For more about reasonable security arrangements, see Power, *supra* note 22.
111 "Privacy Breach Management", *supra* note 67 at 3.
112 *Ibid*.
113 *Ibid*.
114 *Ari* BCCA, *supra* note 41.
115 *Ibid; Privacy Act, supra* note 7.

educational programming. By repealing section 73, and by making unauthorized access and disclosure of that information actionable *per se*, plaintiffs could at least recover nominal damages from the Province.

Lastly, the Commissioner's findings on the Ministry of Health and Ministry of Education breaches weigh heavily in favor of finding that the Province breached a private law duty of care to individuals who suffered loss when it failed to supervise and enforce the protection of personal information at those Ministries. Negligence law is an important legal mechanism for holding the Province accountable to individuals; it should be available to British Columbians when the Province fails to meet its obligations under *FIPPA*.