HEALTH INFORMATION PRIVACY AND THE LAW: NARROWING ALBERTA'S ACCOUNTABILITY GAPS

ERIN NELSON*

Current Alberta law does not adequately respond to violations of health information privacy. While privacy is an ill-defined concept in general, there is no uncertainty as to the importance of privacy in relation to personal health information. The increasing use of electronic means to generate and store health information creates an urgent demand for legal regimes that protect the privacy of health information, and that provide mechanisms to facilitate accountability when privacy is infringed. This author explores health information management, Alberta's current legal landscape in relation to personal information protection, and methods to enhance accountability that can and should be implemented in Alberta.

TABLE OF CONTENTS

I. INTRODUCTION

> Privacy … is a concept in disarray. Nobody can articulate what it means. Currently, privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations.[1]

Privacy has proven to be a challenge for the law to address in a meaningful way, in part because of its breadth and ill-defined nature. There is no dispute that at least some aspects of privacy should be protected by the law, but in the absence of agreement about precisely what privacy means, it is difficult to settle on how to craft law and policy to achieve that objective. In the health information privacy context, however, these conceptual concerns are not in play. There is no uncertainty about what health information privacy entails, and it is

* Professor, Faculty of Law, University of Alberta, Edmonton, Alberta. I would like to thank the anonymous reviewers of this article for their helpful comments.

1 Daniel J Solove, *Understanding Privacy* (Cambridge, Mass: Harvard University Press, 2008) at 1.

therefore more difficult to explain the persistent weaknesses in the law outlined discuss below.

Information and privacy law in Canada is made up of a complex web of legal instruments, including federal and provincial statutes and the common law. The law includes policy to prevent (or at least discourage) privacy breaches, and tools that enable the imposition of legal consequences for privacy-infringing conduct. Given the significant variation among Canadian jurisdictions, it is difficult to speak about information and privacy laws in Canada in general terms. The focus in this article is on privacy law and policy in Alberta, specifically with respect to health information. Although there is no shortage of relevant law, Alberta's privacy regime suffers from some significant limitations. Alberta has three information and privacy statutes that place limits on the collection, use, and disclosure of personal information. One applies to health information specifically, and the other two statutes focus on personal information collected by different kinds of organizations: public bodies and private sector organizations. But Albertans whose personal information is accessed in contravention of these laws may find themselves with no way to hold the wrongdoer accountable. Of the three statutes, only the private sector law provides a private right of action to address violations of privacy, and that right is restricted in nature. Alberta has no statute creating a claim for invasion of privacy in general (as do four Canadian provinces), and our courts have not recognized a common law claim for invasion of privacy, or even the more limited claim for intrusion upon seclusion.

There are significant accountability gaps in Alberta privacy law. The structure of our privacy laws means that public bodies have a weaker incentive than they otherwise might to ensure that their privacy policies, training practices, and other methods of discouraging inappropriate access to and use of personal information are as robust as they can be. It means that individual healthcare providers or staff members who snoop in patient records are not subject to a claim for damages by the person whose information they have accessed. Admittedly, even in jurisdictions with more effective privacy protections, we continue to see instances of unauthorized access, and it is not clear whether existing legal tools are in fact capable of preventing unauthorized access or of creating genuine accountability. That said, the fact that protecting privacy is a challenge should not discourage us from trying to resolve, or at least minimize, these gaps in the law. Put simply, there is much room for improvement in Alberta privacy law.

It is worth noting that the lack of accountability in Alberta around information and privacy laws is not limited to the health information context. In June 2023, the *Globe and Mail* began reporting the results of a lengthy investigation into Canada's freedom of information systems.[2] Entitled "Secret Canada," the series reveals significant concerns with the administration of Canada's access to information laws. Within what the reporters term Canada's "broken" freedom of information (FOI) system, one province stands out as "the government most adept at stonewalling":[3] Alberta. As part of its reporting, the *Globe and Mail* sought to audit how freedom of information requests are handled by Canadian

---

2 "Secret Canada: An Investigation into Canada's Freedom of Information Systems," *The Globe and Mail*, online: [perma.cc/QZ4P-KMDK].

3 Kelly Cryderman, "Alberta Denying Information Requests Is Worrying," *The Globe and Mail* (14 June 2023), online: [perma.cc/BE99-2GYT].

governments. They filed over 250 FOI requests "with every government department and ministry in the country, seeking access to their 2021 internal request tracking systems."[4] The requests asked for data from FOI tracking systems, including "when requests were received and completed and whether any information was provided."[5] Every ministry from every jurisdiction except for Alberta responded by providing the requested information. Alberta, like other Canadian jurisdictions, uses a system to track FOI requests. But provincial officials claimed that because no record existed in the exact format sought by the reporters, the government would need to "create a record" in order to provide the information requested, and that it therefore owed no obligation to comply with the request.[6] The Office of the Information and Privacy Commissioner of Alberta has since opened an investigation into the government's handling of FOI requests.[7]

I begin this article with an explanation of the context of health information management and some examples of significant privacy violations. I then outline the legal landscape related to personal information protection (primarily in Alberta, but drawing on other provinces as well), beginning with the relevant statutes, and then turning to the common law. Lastly, I turn to an exploration of more effective privacy protections that can and should be implemented in Alberta.

II. HEALTH INFORMATION PRIVACY IN CONTEXT

A. HEALTH INFORMATION MANAGEMENT

Participation in almost any aspect of social or economic life requires that we share some personal information. The decision to disclose information is acknowledged as a trade-off in order to continue to be included in many social pursuits, or to be able to access goods and services.[8] Once shared, personal information is vulnerable to unauthorized access. But keeping health information to ourselves is not an option — in order to obtain safe and effective health care, we have no alternative but to reveal information to health care providers.

This is not a new reality. Patients seeking health care have always had to share personal information (such as health history and family history) with their health care providers. What is relatively new is the storage of health information in electronic health records (EHRs). As I explain in more detail below, the risks to information security created by EHRs are significant and difficult to manage.

---

4 Robyn Doolittle & Tom Cardoso, "How Canada's FOI System Broke Under its Own Weight," *The Globe and Mail* (9 June 2023), online: [perma.cc/8UL5-QT6N].

5 Robyn Doolittle & Tom Cardoso, "Alberta's Refusal to Share FOI Data Highlights Gaps in Access to Information," *The Globe and Mail* (12 June 2023), online: [perma.cc/7JTL-9G6V].

6 *Ibid*.

7 Robyn Doolittle & Tom Cardoso, "Alberta's Information Watchdog Opens Systemic Probe into Ministries' Handling of Access Requests," *The Globe and Mail* (2 October 2023), online: [perma.cc/5Q2G-LU7K].

8 Teresa Scassa, "A Human Rights-Based Approach to Data Protection in Canada" in Elizabeth Dubois & Florian Martin-Bariteau, eds, *Citizenship in a Connected Canada: A Research and Policy Agenda* (Ottawa: University of Ottawa Press, 2020) 173 at 175.

Health information is collected, used, disclosed, and produced within the context of provider-patient relationships. Health information is recognized as being extremely sensitive personal information that must be disclosed in order to obtain safe and effective health care.[9] In view of the sensitive nature of this information, health care providers owe legal, professional, and ethical obligations of confidentiality in relation to the health information that is entrusted to them by their patients and may face professional discipline and legal consequences for breaching confidentiality.[10]

Before the introduction of EHRs, patient information was generally collected and stored by the individual providers who played a role in caring for a particular patient. Records, whether electronic or paper-based, were stored by and accessible only to the provider in question. In the modern health care system, health information is increasingly managed electronically, both through electronic medical records (provider-created records that are stored electronically rather than as paper records[11]) and EHRs (a collection of patient health information that includes information from all of the patient's interactions with the health care system,[12] including hospital records, test results, and diagnostic information).

The primary rationale for the adoption of EHRs is the gains that can be made in improving patient safety and efficacy of care by having patient information available at the point of care.[13] To take just one example: a patient's medication history stored in a family doctor's office is no use to the team treating that patient in the emergency department. If the medication history reveals an allergy to a medication that could be used in the context of an emergency, that information is important for the emergency team to know about. At a minimum, having this information could save valuable time and potentially improve the patient's outcome. At best, it could prevent a dangerous or even fatal allergic reaction.

Alberta's EHR is Alberta Netcare. Netcare permits access to Albertans' health information at point of care. Access to Alberta Netcare is afforded to authorized health information custodians for various purposes, including to determine eligibility for health services and to provide health services.[14] The *Health Information Act* (*HIA*) and associated regulations specify that members of several health care professions, including physicians, nurses, optometrists, chiropractors, dentists, midwives, and podiatrists, are custodians of health information, as are hospital boards, nursing home operators, pharmacies, and several other

---

9 As Justice La Forest explained in *McInerney v MacDonald*, [1992] 2 SCR 138 at 152–53 [*McInerney*]: "A doctor is in a better position to diagnose a medical problem if the patient freely imparts personal information. The duty of confidentiality that arises from the doctor-patient relationship is meant to encourage disclosure of information and communication between doctor and patient."

10 See e.g. Canadian Medical Association, *CMA Code of Ethics and Professionalism*, Ottawa: CMA, 2018, arts 18–21, online: [perma.cc/4Z7R-525A] [*CMA Code of Ethics*]; College of Physicians and Surgeons of Ontario, *The Practice Guide: Medical Professionalism and College Policies*, Toronto: CPSO, 2021 at 9, online: [perma.cc/NX3H-A9KR] [*Physicians Practice Guide*]; College of Registered Nurses of Alberta, *Entry Level Competencies for the Practice of Registered Nurses*, Edmonton: CRNA, 2019, art 2.4, online: [perma.cc/5Y23-WZAQ] [*Competencies for Registered Nurses*].

11 See e.g. Patrick Binns, "The Impact of the Electronic Health Record on Patient Safety: An Alberta Perspective" (2004) 5:3 Healthcare Papers 47 at 48.

12 *Ibid*.

13 *Ibid*; see also Nir Menachemi & Taleah H Collum, "Benefits and Drawbacks of Electronic Health Record Systems" (2011) 4 Risk Management & Healthcare Policy 47 at 49–50.

14 *Health Information Act*, RSA 2000, c H-5, ss 56.1–56.8 [*HIA*] (Part 5.1 of the *HIA* spells out the rules applicable to electronic health records); see especially, ss 56.6(1)(b), s 56.1(a) (the *HIA* defines the EHR as "the integrated electronic health information system established to provide shared access by authorized custodians to prescribed health information in a secure environment").

organizations.[15] While not all of these custodians would necessarily have access to Alberta Netcare, it is important to note the scope of potential access.[16] Affiliates of authorized custodians (generally, employees of the custodians) may also have access to the EHR by virtue of their employment relationship.

At the time of writing, Alberta is nearing the end of a years-long process to add an integrated clinical information system (Connect Care) to supplement and improve the functionality of Netcare by making it easier to ensure that Netcare has more complete information. The implementation phase of Connect Care is ongoing, having commenced in 2019.[17] From a provider standpoint, Connect Care should make access to patient information more efficient. Prior to the implementation of Connect Care, Alberta Health Services (AHS, Alberta's province-wide health system) alone used more than 1,300 different information systems to hold patient information.[18] Connect Care will also give patients better access to their health information and improve on existing processes for information sharing between patients and providers. These changes should help to enhance patient safety, by ensuring that all members of the care team have access to accurate and timely information.

The increasing integration of health records offered by the combination of EHRs and clinical information systems like Connect Care provides significant potential benefits. We should see fewer errors in patient care, fewer problematic medication interactions, and better support for clinical decisions and diagnosis. But there are also risks — specifically, risks to the security of the information once it is accessible in one place. The ever-present concern that accompanies the adoption of EHRs is the fact that patient records are available to vast numbers of EHR users, and are therefore susceptible to inappropriate use, including everything from accidental access to deliberate snooping. The potential for misuse of information is sought to be managed in various ways: the purposes for which health information may be accessed are limited to those specified in the *HIA*. Numerous safeguards are in place, including physical safeguards (for example, alarm systems, secure storage, and secure wireless access), administrative safeguards (including privacy policies, training on the use of the system, unique user-identifiers, periodic audit log review, and logout requirements), and technical safeguards (such as encryption, firewalls, intrusion detection, and anti-virus software).[19] In spite of the limits spelled out in the *HIA* and the above-noted safeguards, the privacy-related risks created by the use of EHRs have proven to be difficult to manage, and instances of unauthorized access continue to occur.

---

15 *Ibid*, s 1(1); *Health Information Regulation*, Alta Reg 70/2001, s 2.

16 Not all health information custodians are automatically able to access the EHR. Custodians must meet the eligibility requirements spelled out in the *Alberta Electronic Health Record Regulation*, Alta Reg 118/2010 to gain access to Alberta Netcare.

17 Implementation has been delayed by the pandemic. The current plan is to have the final phase of implementation begin in late 2024. Taylor Lambert, "Connect Care Was Supposed to Revolutionize Alberta Health Services. Then Came the Pandemic," *CBC News* (30 October 2022), online: [perma.cc/R24N-KQ2U].

18 Daniel C Baumgart, "Digital Advantage in the COVID-19 Response: Perspective from Canada's Largest Integrated Digitalized Healthcare System" (2020) 3 npj Digital Medicine.

19 See e.g. Office of the National Coordinator for Health Information Technology, "Safer Guides" (28 November 2018), online: *HealthIT* [perma.cc/VJ9E-9SM9]; Roger Collier, "New Tools to Improve Safety of Electronic Health Records" (2014) 186:4 CMAJ 251; Office of the Information and Privacy Commissioner of Alberta, "Guidance for Electronic Record Systems" (2016), online (pdf): [perma.cc/5XQG-2KCY].

The need to provide broad and integrated access to EHRs while also protecting privacy is not a new problem, but it remains a problem in want of a solution. In the section that follows, I provide several examples of unauthorized access to health information in order to contextualize the discussion of accountability gaps in existing health information laws.

B. UNAUTHORIZED ACCESS TO HEALTH INFORMATION

Privacy infringements in the health care context are increasingly common in Alberta. Hundreds of breaches of the *HIA* have been reported in the Annual Reports of the Office of the Information and Privacy Commissioner (OIPC) over the past several years.[20] While many of these breaches likely result from inadvertent errors, some are intentional and have resulted in convictions for contraventions of the *HIA*.[21] Below, I outline some significant privacy breaches in Alberta and elsewhere in Canada in order to provide a clear sense of the vulnerability of health information to inappropriate access.

Kirk McEwing spent several weeks in hospital in 2014, being treated for a serious illness. A few years later, he heard some acquaintances discussing his health history. He requested Netcare audit logs and discovered that the wife of a long-time friend of his had accessed his health information without authorization. The individual who accessed McEwing's records was at the time employed as an assistant, and the designated privacy officer, in a physician's office. She reviewed "discharge summaries that featured detailed descriptions of his illness, treatment plan and medications."[22]

McEwing complained to the OIPC, and the OIPC agreed that there were grounds for an *HIA*-based prosecution of the individual who had accessed his records. However, the (then in-place) two-year limitation period had already expired, meaning that there could be no prosecution.[23] According to a news story about the incident, the individual who

---

20 In its 2021/22 Annual Report, the Office of the Information and Privacy Commissioner (OIPC) notes that 551 breaches of the *HIA* were reported by custodians to the OIPC (Alberta, Office of the Information and Privacy Commissioner, *Annual Report 2021-22* (Edmonton: Office of the Information and Privacy Commissioner, 2022) at 41, online: [perma.cc/Z63C-DLGV]). This is substantially lower than the 930 reported in 2020 to 2021. For context, 938 breaches were reported in 2019/20, and 674 in 2018/19. The significant increase between 2018/19 and 2019/20 likely reflects an amendment to the *HIA* requiring custodians to report "any loss of individually identifying health information or any unauthorized access to or disclosure of individually identifying health information in the custody or control of the custodian if there is a risk of harm to an individual as a result of the loss or unauthorized access or disclosure" (*HIA*, *supra* note 14, s 60.1(2); Alberta, Office of the Information and Privacy Commissioner, *Annual Report 2019-20* (Edmonton: Office of the Information and Privacy Commissioner, 2020), online: [perma.cc/7QVD-MXAC]). The mandatory breach-reporting requirement came into force on August 31, 2018 (see Alberta, Office of the Information and Privacy Commissioner of Alberta, *Annual Report 2018-19* (Edmonton: Office of the Information and Privacy Commissioner, 2019) at 18, online: [perma.cc/D5HR-KSM4]).

21 *Annual Report 2021-22*, *ibid* at 42: the Office of the Privacy Commissioner of Alberta notes that, as of 31 March 2022, there have been 21 convictions under the offence provisions in the *HIA* (for accessing and/or disclosing health information in contravention of the *HIA*). The two convictions for unauthorized access to health information described in the 2021/22 Annual Report each involved numerous instances of accessing information of multiple individuals (one individual accessed information 76 individuals 238 times over two years, the other accessed information of 189 individuals 985 times over a period of two years).

22 Keith Gerein, "Victim 'Furious' over Health-Record Snooping Wants Changes to Alberta's Prosecution Limit," *The Edmonton Journal* (15 August 2018), online: [perma.cc/P77T-ZZ9K].

23 At the time of McEwing's complaint, a prosecution could be commenced within two years of the commission of the alleged offence (see *Health Information Amendment Act*, SA 2006, c 18, s 17, adding section 107(8) to the *HIA*). In 2020, the *HIA* was amended (*Health Statutes Amendment Act, 2020 (No.2)*, SA 2020, c 35). Section 107(8) was repealed. The new limitation period states that a prosecution

inappropriately accessed McEwing's records went on to work for AHS and had Netcare access as part of her role with the organization.[24]

In 2015, the OIPC investigated a number of alleged violations of the *HIA* at the Calgary South Health Campus emergency department. A patient was treated in the department and flagged as a "confidential" patient.[25] The investigation revealed that 49 members of staff had accessed the patient's information inappropriately or outside their role, in that they were not involved in the provision of health care to the patient. Most offered no justification for having reviewed the patient's health care information, while some explained that they viewed the information out of curiosity.

The patient was Christine Hagan. Christine was dying of pancreatic cancer. She gave a lethal dose of drugs to her daughter, Jessica, who had Down Syndrome. Jessica was found dead in the home she shared with her mother; Christine was found in medical distress and brought to the emergency department at South Health Campus. Family members learned of the privacy breach via the media.[26]

All of the employees found to have accessed the patients' health information inappropriately were disciplined by AHS, but the discipline decisions were reversed in 38 of the 49 cases (and the sanctions reduced in the remaining 11) after the employees' unions filed grievances. The OIPC investigation report notes that "a contributing factor in the need to reduce or rescind discipline for the unauthorized access that occurred was due to the significant gaps by AHS in ensuring its affiliates were aware of their responsibilities and in the failure to implement related safeguards."[27] The OIPC found that AHS had appropriate administrative safeguards in place to protect the confidentiality of health information, but that it had failed to establish necessary technical safeguards or to monitor the existing safeguards. In addition, while AHS had policies and training in place, it "did not take reasonable steps to ensure the policies were known, understood, applied and monitored."[28]

In a report published in 2018, the Privacy Commissioner for Nova Scotia describes an investigation into the conduct of a pharmacist who had, over a two-year period, inappropriately used Nova Scotia's Drug Information System (DIS) to view personal health information of 46 different individuals.[29] The DIS is a province-wide database containing identifying information (name, date of birth, and gender), as well as prescription history, medical conditions, and other health information.[30] The DIS can be accessed by staff at

---

may be commenced "within 2 years after the day on which evidence of the alleged offence first came to the attention of the Commissioner" (*HIA*, *supra* note 14, s 107(9)).

24 Gerein, *supra* note 22.

25 Alberta, Office of the Information and Privacy Commissioner of Alberta, *Investigation Report H2017-IR-02: Investigation into Multiple Alleged Unauthorized Accesses of Health Information at South Health Campus* (Edmonton: Office of the Information and Privacy Commissioner, 2017) at para 84, online: [perma.cc/G3MX-A5RL] [*Investigation Report H2017-IR-02*].

26 CBC News, "Privacy Breach, AHS Secrecy and Lack of Firings an 'Additional Blow' to Christine Hagan's Family," *CBC News* (15 January 2016), online: [perma.cc/J3XG-TR6H].

27 *Investigation Report H2017-IR-02*, *supra* note 25 at para 84.

28 *Ibid* at para 75.

29 Nova Scotia, Office of the Information and Privacy Commissioner for Nova Scotia, *Investigation Report IR18-02: Drug Information System Privacy Breaches Sobeys National Pharmacy Group* (Halifax: Office of the Information and Privacy Commissioner for Nova Scotia, 2018) at para 3, online: [perma.cc/6BXU-D368] [*Investigation Report, Sobeys Privacy Breaches*].

30 *Ibid* at para 22.

pharmacies for patients for whom the pharmacy has a "user profile."[31] The Privacy Commissioner concluded that the pharmacist gained access to health information from the DIS for numerous individuals who were not clients of the pharmacy, and that she had done so by creating user profiles for some of them. This allowed the pharmacist to view DIS information about several people, including:

> [H]er child's girlfriend and her parents; her child's friends and acquaintances; an individual she had been involved in a car accident with; her child's teachers and former teachers; her former teacher (deceased); relatives (including deceased relatives); her and her family's health care providers; a former high school classmate who had recently suffered a significant illness; and co-workers.[32]

The Privacy Commissioner's investigation report notes that the investigation confirmed details with respect to a number of the privacy breaches. For example, the report states that an employee "witnessed the pharmacist access the DIS … and then call her spouse … to discuss what she had discovered. The employee heard the pharmacist say that their child cannot see this person because of the medications she and her parent were on."[33] The report also notes that the pharmacist was observed by an employee to "look up DIS profiles after a Prescription Monitoring Profile alert was received.… The employee observed the pharmacist make notes about what was viewed and then call her spouse … to determine if the subject of the alert was someone known to them socially."[34] These are just two incidents among a fairly lengthy list.[35]

In another recent example, the Privacy Commissioner of Saskatchewan investigated complaints about unauthorized access to health information by a physician who viewed the health information of a number of family members of his child's schoolmate. None of the family members were patients of the physician, and the Privacy Commissioner concluded that the access was unauthorized. The physician accessed the information on dates that coincided with visits by the physician's child to the home of the complainant family members.[36]

In Alberta, we have also had reports of access to health information by political actors. In May 2020, the Alberta government announced planned changes that would limit physician billings to 65 patients per day. Physicians would be paid the full amount per visit for the first 50 patients, and 50 percent of the typical amount for the next 15 patients. A group of pediatricians in Edmonton claimed that these planned changes would have significant negative effects on patient care.[37] The pediatricians explained that this change would force them to divert patients to hospital emergency rooms for care that the clinic had to that point been able to provide. On Twitter and in statements to the media, the Minister of Health's press secretary and issues manager both commented that the clinic would not suffer any loss

---

31 *Ibid* at para 23.
32 *Ibid* at para 29.
33 *Ibid* at para 43.
34 *Ibid*.
35 *Ibid*.
36 Saskatchewan, Office of the Saskatchewan Information and Privacy Commissioner, *Investigation Report 065-2021, 068-2021, 069-2021, 073-2021* (Regina: Office of the Saskatchewan Information and Privacy Commissioner, 2021) at paras 9–13, online: [perma.cc/C6E6-WRTV].
37 Ashley Joannou, "Edmonton Pediatrician Warns of Service Cuts Thanks to Changes Billing," *The Edmonton Journal* (28 April 2020), online: [perma.cc/3FN3-M6R8].

of revenue, because a review of the clinic's billing information showed that the clinic does not see 50 patients per day, per physician.[38]

The Minister's staff acknowledged that they accessed clinic billing information in order to reach this conclusion.[39] Billing information is health information according to the *HIA*.[40] The *HIA* permits the Minister of Health to access health information for a variety of purposes, including to inform health system management and health policy development, and so it is arguable that the Minister's use of billing information is authorized by the law, at least in some circumstances.[41] But even if the Minister's office can argue that the information was accessed for reasons related to health system management or policy development and therefore in keeping with the letter of the law, it is extremely troubling to see government officials seek to excuse a politically motivated use of health information on this basis.

As the Privacy Commissioner for Nova Scotia has explained, unauthorized access to personal health information persists, despite the existence of legal rules and professional standards that leave no room for uncertainty around the impropriety of this conduct:

> It bears repeating in the context of this investigation report that the risk of authorized users engaging in unauthorized access of personal health records is a significant and foreseeable risk for any health information custodian. Even despite professional ethical standards, policies and training, some individuals continue to operate with a total disregard for the privacy of the individuals served by the health care system. Trust for custodians and the health care system in general is damaged when custodians do not appreciate the constant risk from authorized users abusing their authority. As electronic records and broad access to health information proliferates, the nature of this risk continues to augment.[42]

These examples reveal real and substantial risks to health information privacy. In the next section, I describe the law related to health information, noting gaps that lead to questions about accountability when the security of health information is not maintained.

III. THE LEGAL LANDSCAPE: PRIVACY PROTECTION IN LEGISLATION AND THE COMMON LAW

The collection, use, and disclosure of personal information is governed by several federal, provincial, and territorial statutes. There are also common law claims that can arise when privacy is violated, and ethical and professional obligations relating to confidentiality of health information specifically.[43] The result is an overlapping, sometimes confusing, set of rules that can vary depending on what kind of institution is collecting personal information, what kind of personal information is being collected, and where in Canada the information is being collected.

---

38 Charles Rusnell, "Second Privacy Breach Complaint Filed Against Alberta Health Minister Tyler Shandro," *CBC News* (11 May 2020), online: [perma.cc/7BUW-TFKL].

39 *Ibid*.

40 *HIA*, *supra* note 14, s 1(1)(k) (defining "health information"), s 1(1)(u) (defining "registration information").

41 *Ibid*, s 27(2).

42 *Investigation Report, Sobeys Privacy Breaches*, *supra* note 29 at para 70.

43 See e.g. *McInerney*, *supra* note 9; *CMA Code of Ethics*, *supra* note 10; *Physicians Practice Guide*, *supra* note 10; *Competencies for Registered Nurses*, *supra* note 10.

In this section, I provide an overview of the various legal tools that relate to the governance of health information, including the statutes that govern the collection, use, and disclosure of health information, and the common law claims that can arise when privacy is violated. Information and privacy law is complex; the objective of this section is to provide a high-level overview of the relevant statutes and how they overlap and interact in relation to health information. This discussion is not intended to be exhaustive. There is a vast literature available for readers who are interested in a comprehensive discussion of information and privacy laws in Canada.[44]

A. STATUTES

1. INFORMATION AND PRIVACY LAWS

The collection, use, and disclosure of personal information is regulated in slightly distinct ways depending on the nature of the organization that collects the information. Information and privacy laws in Canada create two broad categories of organizations: public bodies (including government agencies, municipalities, school boards, post-secondary educational institutions, and hospitals)[45] and private organizations (including associations, partnerships, persons, and trade unions).[46]

a. Public Sector Laws

The collection, use, and disclosure of personal information held by public bodies is governed by freedom of information and protection of privacy laws. Each province and territory has such a statute,[47] and federal legislation governs privacy and access to information in relation to information in the control of federal government institutions.[48]

Access to information laws have been a feature of the Canadian legal landscape since the adoption of the *Access to Information Act* by the federal government in 1983.[49] All Canadian provinces and territories adopted legislation governing access to information and privacy between 1977 and 2002.[50] The major objectives of access to information and privacy laws are to permit access to records (subject to some exceptions) in the custody or control of

---

44 For an in-depth discussion of privacy and information law in Canada, see Barbara von Tigerstrom, *Information & Privacy Law in Canada* (Toronto: Irwin Law, 2020) [von Tigerstrom, *Information & Privacy Law*]. Other resources include: Mike Larsen & Kevin Walby, eds, *Brokering Access: Power, Politics, and Freedom of Information Process in Canada* (Vancouver: UBC Press, 2012); Kris Klein et al, *The Law of Privacy in Canada* (Toronto: Carswell, 2004).

45 *Freedom of Information and Protection of Privacy Act*, RSA 2000, c F-25, ss 1(p), 1(j), 1(g) [*FOIP Act*].

46 *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, s 2(1) ("organization") [*PIPEDA*].

47 See e.g. *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165; *Access to Information and Protection of Privacy Act*, SNWT 1994, c 20; *The Freedom of Information and Protection of Privacy Act*, SM 2021, c 43; *Freedom of Information and Protection of Privacy Act*, RSO 1990, c F.31; *Right to Information and Protection of Privacy Act*, SNB 2009, c R-10.6; *FOIP Act*, *supra* note 45; *The Freedom of Information and Protection of Privacy Act*, SS 1990-91, c F-22.01.

48 *Access to Information Act*, RSC 1985, c A-1 [*Canada Access to Information Act*]; *Privacy Act*, RSC 1985, c P-21 [*Canada Privacy Act*].

49 *Canada Access to Information Act*, *ibid*. The *Canada Privacy Act*, *ibid*, was also adopted at the same time. See also Ann Rees, "Sustaining Secrecy: Executive Branch Resistance to Access to Information in Canada" in Larsen & Walby, *supra* note 44, 35 at 38.

50 Gary Dickson, "Access Regimes: Provincial Freedom of Information Law Across Canada" in Larsen & Walby, *ibid*, 68 at 68.

public bodies, and to control the manner in which a public body may collect, use, and disclose personal information.[51]

The *Freedom of Information and Protection of Privacy Act*[52] was the first information and privacy statute to be adopted in Alberta. The *FOIP Act* applies to records in the custody or control of public bodies, including government departments and agencies, universities and other post-secondary educational institutions, school boards, hospitals, and other health care bodies.[53] The main relevance of the *FOIP Act* in the health information context is in relation to records held by hospitals or other health care bodies.

b. Private Sector Laws

In addition to privacy and access to information laws, all Canadian jurisdictions have legislation providing for the appropriate collection, use, and disclosure of personal information by private sector organizations.[54]

The federal statute governing personal information in the private sector is the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*).[55] *PIPEDA* was adopted in 2000 in response to the substantial increase in electronic data collection (and the immense potential for abuse of that information) that accompanied a rapidly expanding e-commerce system.[56] *PIPEDA* (like other private sector information legislation) seeks to strike a balance between individual privacy interests and "the needs of businesses to collect, use, and disclose personal information."[57]

PIPEDA applies to personal information — including health information — that is "collected, used, or disclosed in the course of commercial activities."[58] The Act applies to some extent in every jurisdiction in Canada, in that it applies to all businesses operating in Canada where the business makes use of personal information that crosses provincial or national borders, and to all federally regulated commercial organizations.[59] Where a province has "substantially similar" legislation that applies to an organization or activity, that organization or activity can be exempted from the application of *PIPEDA*, and the provincial

---

51 See e.g. *FOIP Act*, *supra* note 45, ss 2(a)–(b).

52 *Ibid*.

53 *Ibid*, ss 1(p), 1(j), 1(g), defining "public body," "local public body," and "health care body," respectively.

54 *PIPEDA*, *supra* note 46; *Personal Information Protection Act*, SBC 2003, c 63; *Personal Information Protection Act*, SA 2003, c P-6.5 [*PIPA*]; *Act Respecting the Protection of Personal Information in The Private Sector,* CQLR c P-39.1 [*Private Sector Information Protection Act*]. In provinces without a law that has been deemed "substantially similar" to *PIPEDA*, the federal law applies.

55 *PIPEDA*, *ibid*.

56 Mahmud Jamal, "Is PIPEDA Constitutional?" (2006) 43:3 Can Bus LJ 434 at 435. As Jamal (now Justice Jamal) has explained, "PIPEDA's rules protect personal information both as an end in itself and as a means for fostering an environment in which Canadian consumers have trust and confidence in the electronic marketplace. The government of Canada viewed fostering consumer confidence and trust as essential for the Internet's full potential to be realized."

57 Scassa, *supra* note 8 at 175. See also Jamal, *ibid*; *PIPEDA*, *supra* note 46, s 3.

58 von Tigerstrom, *Information & Privacy Law*, *supra* note 44 at 455.

59 Canada, Office of the Privacy Commissioner of Canada, *The Application of PIPEDA to Municipalities, Universities, Schools, and Hospitals* (16 December 2015), online: [perma.cc/AM9Y-ET24] [OPCC, *Application of PIPEDA*] (Organizations within Canada's three territories (the Northwest Territories, Yukon, and Nunavut) are considered federally regulated organizations, and so *PIPEDA* applies to those organizations).

statute will apply instead.[60] Alberta, British Columbia, and Quebec have provincial private sector information legislation that has been deemed "substantially similar" to *PIPEDA*, and those provincial laws therefore apply to organizations operating within these provinces.[61] In some provinces, health information legislation has been deemed "substantially similar" to *PIPEDA*, meaning that the provincial health information law applies to health information in the private sector.[62] *PIPEDA* governs the collection, use, and disclosure of personal information (including health information) in the private sector in Saskatchewan, Manitoba, Prince Edward Island, and all three territories.

In jurisdictions where *PIPEDA* applies to health information, it governs the collection, use, and disclosure of personal information "in the course of commercial activities."[63] In the health care context, this would capture private health care practices (even those that are publicly funded), but not hospitals or other public facilities.[64]

2. HEALTH INFORMATION LAWS

As personal information that may be within the control of a public body, or collected by privately owned and operated businesses, health information can fall under both *FOIP* and private sector regimes. Most provinces and territories also have legislation specific to the collection, use, and disclosure of health information; in these jurisdictions, health information statutes are the principal source of governance for personal health information." Health information laws are in place in Alberta, Saskatchewan, Manitoba, Ontario, New Brunswick, Nova Scotia, Newfoundland and Labrador, Prince Edward Island, the Yukon, and the Northwest Territories.[65]

---

60 *PIPEDA*, *supra* note 46, ss 25–26 (section 25(1) provides that the Privacy Commissioner shall submit an annual report indicating "the extent to which the provinces have enacted legislation that is substantially similar to this Part and the application of any such legislation," and section 26(2)(b) provides for the Governor in Council to order that the relevant organizations or activities be exempted from the application of *PIPEDA*).

61 *Organizations in the Province of Alberta Exemption Order*, SOR/2004-219; *Organizations in the Province of British Columbia Exemption Order*, SOR/2004-220; *Organizations in the Province of Quebec Exemption Order*, SOR/2003-374.

62 Ontario, New Brunswick, Newfoundland & Labrador, Nova Scotia: *Health Information Custodians in the Province of Ontario Exemption Order*, SOR/2005-399; *Personal Health Information Custodians in New Brunswick Exemption Order*, SOR/2011-265; *Personal Health Information Custodians in Newfoundland and Labrador Exemption Order*, SI/2012-72; *Personal Health Information Custodians in Nova Scotia Exemption Order*, SOR/2016-62.

63 *PIPEDA*, *supra* note 46, s 4(1)(a).

64 OPCC, *Application of PIPEDA*, *supra* note 59 (the public facilities are subject to FOIP laws, as explained above).

65 *HIA*, *supra* note 14; *The Personal Health Information Act*, CCSM c P33.5 [*PHIA* Man]; *The Health Information Protection Act*, SS 1999, c H-0.021 [*HIPA* Sask]; *Personal Health Information Protection Act 2004*, SO 2004, c 3 [*PHIPA* ON]; *Personal Health Information and Privacy Act*, SNB 2009, c P-7.05; *Personal Health Information Act*, SNS 2010, c 41; *Personal Health Information Act*, SNL 2008, c P-7.01; *Health Information Act*, RSPEI 1988, c H-1.41 [*HIA* PEI]; *Health Information Privacy and Management Act*, SY 2013, c 16; *Health Information Act*, SNWT 2014, c 2. Nunavut does not have a health information law, and so health information is governed by the *Access to Information and Protection of Privacy Act*, CSNu, c A-20 (public sector) and *PIPEDA*, *supra* note 46 (private sector). In Quebec, health information is governed by provincial public and private sector information laws (*Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information*, CQLR c A-2.1; *Private Sector Information Protection Act*, *supra* note 54). British Columbia has an "E-Health" act, which is aimed at databases of information in custody or control of health care bodies: *E-Health (Personal Health Information Access and Protection of Privacy) Act*, SBC 2008, c 38.

While there are some variations among health information statutes, the laws share similar features. All of these laws apply to "identifying health information," although the statutes define "identifying health information" somewhat differently. In Alberta, "health information" is defined as "diagnostic, treatment and care information" or "registration information," or both.[66] These phrases are further defined in the statute, with "registration information" meaning information about individual demographics (including the person's personal health number), contact information, eligibility for health care services, and billing information.[67] Diagnostic, treatment, and care information includes information about a person's physical or mental health, as well as any health services provided to the person, prescription medications, and medical devices or equipment.[68] "Individually identifying health information," in turn, is health information from which the "the identity of the individual who is the subject of the information can be readily ascertained."[69] Some provinces, by contrast, define "identifying health information" as information from which it is reasonably foreseeable that the person could be identified.[70]

Alberta's *HIA* prohibits the collection,[71] use,[72] and disclosure[73] of health information except in accordance with the provisions of the *HIA*.[74] Broadly speaking, the *HIA* requires custodians to protect health information that is in their custody or control.[75] It requires that custodians only collect, use, and disclose health information to the extent necessary to achieve the purpose for which the information was provided to the custodian.[76] The *HIA* specifies that health information should be collected only if it is essential to the intended purpose,[77] that it should be collected with the highest degree of anonymity,[78] and that it should be collected directly from the individual to whom it pertains.[79] The purposes for which health information may be used are limited by the *HIA*, and include the following: providing health care services; determining whether a person is eligible for health services; conducting investigations; discipline proceedings and practice reviews; conducting research; providing education to health care providers; and managing the custodian's operations.[80] Disclosure of health information to third parties is based on the general rule that information

---

66 *HIA*, *ibid*, s 1(1)(k).
67 *Ibid*, s 1(1)(u).
68 *Ibid*, s 1(1)(i).
69 *Ibid*, s 1(1)(p). See also *PHIA* Man, *supra* note 65, s 3, providing that the Act "does not apply to statistical health information, or to health information that does not, either by itself or when combined with other information available to the holder, allow an individual to be readily identified."
70 See e.g. *PHIPA* ON, *supra* note 65, s 4(2); *HIPA* Sask, *supra* note 65, s 3(2), which provides that the *Act* "does not apply to: (a) statistical information or de-identified personal health information that cannot reasonably be expected, either by itself or when combined with other information available to the person who receives it, to enable the subject individuals to be identified." See also *HIA* PEI, *supra* note 65, s 1(o).
71 *HIA*, *supra* note 14, s 18.
72 *Ibid*, s 25.
73 *Ibid*, s 31.
74 Non-identifying health information can be collected, used, or disclosed for any purpose. *Ibid*, ss 19, 26, 31.
75 *Ibid*, s 60.
76 *Ibid*, s 58. Section 27 lists the purposes for which health information may be used by custodians.
77 *Ibid*, s 58.
78 *Ibid*, s 57.
79 *Ibid*, s 22(1). Section 22(2) provides for indirect collection of health information in certain circumstances.
80 *Ibid*, s 27(1). Certain custodians including AHS, the Minister of Health, and certain provincial health boards are also permitted to use health information for planning and management of the health system, public health surveillance, and in health policy development (*ibid*, s 27(2)).

can be disclosed with the consent of the person whose information it is, although the *HIA* includes numerous exceptions to the requirement of consent.[81]

It is an offence to "knowingly … collect, use, disclose or create health information in contravention of this Act," and to "gain or attempt to gain access to health information in contravention of this Act."[82] A person who gains (or attempts to gain) access to health information for a purpose that is not outlined in the *HIA* contravenes the *HIA* and can be convicted of an offence and may be required to pay a fine.[83]

One key feature that almost all Canadian health information statutes (including Alberta's) lack is a provision that creates a private right of action for breaches of the statute. Ontario is the only Canadian jurisdiction whose *Personal Health Information Protection Act* (*PHIPA*) includes such a provision.[84] The remedy provided by the Ontario statute is limited — damages may be awarded for "actual harm" suffered as a result of a violation of the Act, and are available only in situations where the privacy commissioner's order is final, or where the defendant has been convicted of an offense under *PHIPA*.[85] In cases where the defendant or defendants acted "wilfully or recklessly" in breaching *PHIPA*, the damages award may include up to $10,000 for mental anguish.[86]

It is clear that accessing health information for reasons that do not correspond to a purpose articulated in the *HIA* is prohibited. However, there is no practical way to authorize access to health information by vast numbers of users and, at the same time, to prevent all inappropriate access to that information. As the examples of unauthorized access provided above illustrate, such inappropriate access occurs despite the restrictions articulated in the *HIA*. Ultimately the system depends on the good behaviour of those with access to health information by virtue of their role within the health care system.

When a health information custodian or affiliate fails to meet that standard of good behaviour, what legal avenues remain? Generally, when someone is injured by the actions of another, the injured party can seek relief from the courts, typically via a tort claim. The focus of the next section is on the role of tort of law in providing remedies for violations of privacy.

B. TORT LAW: REMEDIES FOR INVASIONS OF PRIVACY

The statutory regimes described above are focused on restricting the circumstances within which personal information is collected, used, and disclosed with a view to maintaining the security of personal information held by others. But as is clear from the examples of unauthorized access referred to above, those laws are not sufficient on their own to ensure that personal information is not misused. When personal information is used or accessed in a manner that contravenes the law, what remedial options does the victim have?

---

81 *Ibid*, ss 35–40.
82 *Ibid*, s 107(2).
83 *Ibid*, s 107(6). The fines are significant — for individuals, the maximum fine is $200,000, for "any other person," up to $1,000,000.
84 *PHIPA* ON, *supra* note 65, s 65.
85 *Ibid*, ss 65(1)–(2).
86 *Ibid*, s 65(3). See also von Tigerstrom, *Information & Privacy Law*, *supra* note 44 at 487.

A few Canadian provinces have legislation that creates a tort claim for "invasion of privacy." The *Privacy Acts* of British Columbia, Saskatchewan, Manitoba, and Newfoundland and Labrador all establish a cause of action for invasion of privacy,[87] which is committed when "a person wilfully and without claim of right, … violate[s] the privacy of another person."[88] The torts have been judicially considered, albeit not in a manner that has yielded a clear and consistent approach to determining what kinds of conduct will amount to an invasion of privacy.[89] That said, it does seem clear that the statutory torts would provide an avenue for compensation for those whose health information has been inappropriately accessed.[90] Alberta law does not include a claim of this nature, meaning that such a claim is not available to address instances of unauthorized access to health information in the province.[91]

In absence of a generally applicable claim for invasion of privacy, we can look to other information and privacy legislation for statutory claims. For example, Ontario's *PHIPA* creates a private right of action for violations of the Act, as does Alberta's *Personal Information Protection Act* (the private sector information and privacy law in Alberta).[92] Alberta's *HIA*, as noted, does not provide for a private right of action.

Canadian common law does not include a discrete tort claim for "breach of statute,"[93] meaning that in the absence of a private remedy in health information legislation, there is no statute-based tort claim available to persons whose health information has been used in a manner that contravenes the *HIA*. The only route to a claim for damages for inappropriate use of or access to health information in Alberta is on the basis of an existing common law tort claim.[94] Several torts exist that can, in some circumstances, protect some aspects of privacy, but most are not well-suited to claims of privacy infringements that involve inappropriate access to health records.[95]

---

87 *Privacy Act*, RSBC 1996, c 373, s 1(1) *Privacy Act* BC]; *Privacy Act*, RSS 1978, c P-24 [*Privacy Act* Sask], s 2; *Privacy Act*, CCSM c P125, s 2(1) [*Privacy Act* Man]; *Privacy Act*, RSNL 1990, c P-22, s 3(1) [*Privacy Act* NL].

88 *Privacy Act* Sask, *ibid*, s 2.

89 Chris DL Hunt & Nikta Shirazian, "Canada's Statutory Privacy Torts in Commonwealth Perspective" (2016) Oxford University Comparative L Forum 3 at 2, online: [perma.cc/G6CH-THLD] [Hunt & Shirazian, "Statutory Privacy Torts"].

90 See e.g. *Bierman v Haidash*, 2021 SKQB 44 at para 52 ("in this instance, Dr. Haidash accepted in a written statement submitted to the College of Physicians and Surgeons that he accessed personal health information without a legitimate need to know the information and without consent. This admission cannot be viewed as anything but a violation of Ms. Bierman's reasonable expectation of privacy"); *Hynes v Western Regional Integrated Health Authority*, 2014 NLTD 137 [*Hynes*].

91 For a detailed discussion of the statutory claim for invasion of privacy see Hunt & Shirazian, "Statutory Privacy Torts," *supra* note 89; Chris DL Hunt, "Reasonable Expectations of Privacy in Canadian Tort Law" (2018) 84 SCLR (2d) 269 [Hunt, "Reasonable Expectations"]; von Tigerstrom, *Information & Privacy Law*, *supra* note 44 at 71–93.

92 *PIPA*, *supra* note 54. As noted above, both of these claims are limited in that they require the plaintiff to establish "actual harm" as a result of a violation of the *AB PIPA* and are available only in situations where commissioner's order is final, or where the defendant has been convicted of an offense under the relevant legislation. *PHIPA* ON, *supra* note 65, s 65; *PIPA*, *supra* note 54, s 60 (here, the wording is slightly different, providing that a person may seek damages "for loss or injury that the individual has suffered as a result of the breach by the organization of obligations under this Act or the regulations").

93 *The Queen (Can) v Saskatchewan Wheat Pool*, [1983] 1 SCR 205 [*Saskatchewan Wheat Pool*].

94 *Ibid* at 222–23, 227: As the Supreme Court explained in *Saskatchewan Wheat Pool*, a breach of statute may be evidence of negligence in a negligence claim related to the breach but does not itself ground a claim for damages.

95 These include: intentional infliction of mental distress, breach of confidence, defamation, and nuisance. See e.g. *Roth v Roth* (1991), 4 OR (3d) 740 (ONSC Gen Div); *ES v Shillington*, 2021 ABQB 739 [*Shillington*]. See also Lewis Klar & Cameron Jefferies, *Tort Law*, 7th ed (Toronto: Thomson Reuters, 2023) at 102–103.

One option for persons whose health information has been accessed inappropriately is to pursue a negligence claim, given the flexible and broad nature of that claim. As others have noted, however, the structure of the negligence claim itself poses some obstacles to success.[96] Given the deliberate nature of many invasions of privacy, these claims might not be best approached on the basis of the tort of negligence, which is aimed at careless (or unreasonable) rather than intentional conduct. A more significant impediment is the requirement of proof of harm as a result of the negligent conduct.[97] While learning that someone has violated their privacy will likely cause distress, it might be a challenge for the claimant to prove that they have suffered a type of harm recognized as compensable by the law. As Chief Justice McLachlin (as she then was) explained in *Mustapha v. Culligan of Canada Ltd.*:

> Personal injury at law connotes serious trauma or illness: … The law does not recognize upset, disgust, anxiety, agitation or other mental states that fall short of injury. I would not purport to define compensable injury exhaustively, except to say that it must be serious and prolonged and rise above the ordinary annoyances, anxieties and fears that people living in society routinely, if sometimes reluctantly, accept…. Quite simply, minor and transient upsets do not constitute personal injury, and hence do not amount to damage.[98]

If a plaintiff cannot establish that they have suffered a personal injury as a result of a violation of their privacy, they may be able to demonstrate economic loss — such as the costs incurred in taking steps to better safeguard their personal information.[99] Plaintiffs seeking to recover claims for economic harm alone will be unlikely to succeed unless they are able to fit their claim within a recognized category of recoverable economic loss.[100] All of this suggests that the negligence claim might not be a particularly effective or efficient way for a victim of a health information privacy breach to seek compensation.

The most obvious type of tort claim for a plaintiff to pursue when their health information is used or accessed improperly is one based on invasion of privacy — either a general claim for invasion of privacy, or the specific privacy-related claim for intrusion upon seclusion, which has been recognized in some Canadian jurisdictions.[101] The claim for intrusion upon

---

96 See e.g. Barbara von Tigerstrom, "Direct and Vicarious Liability for Tort Claims Involving Violation of Privacy" (2018) 96:3 Can B Rev 539 [von Tigerstrom, "Direct and Vicarious Liability"].

97 *Mustapha v Culligan of Canada Ltd*, 2008 SCC 27 at para 3 [*Mustapha*].

98 *Ibid* at para 9 [citations omitted].

99 von Tigerstrom, "Direct and Vicarious Liability," *supra* note 96 at 551. As von Tigerstrom notes, these costs could include monitoring one's finances to ensure that their personal information has not been used by someone else to secure credit in their name.

100 See e.g. *1688782 Ontario Inc v Maple Leaf Foods Inc*, 2020 SCC 35 at para 19 ("[w]hile this Court has recognized that pure economic loss may be recoverable in certain circumstances, there is no general right, in tort, protecting against the negligent or intentional infliction of pure economic loss.") See also von Tigerstrom, "Direct and Vicarious Liability," *ibid* at 551–52. It is also worth noting that plaintiffs seeking to recover damages from a government body in a negligence claim may face a challenge in establishing that a duty of care is owed, although this is less likely in the case of hospitals and health care facilities than other public authorities: von Tigerstrom, "Direct and Vicarious Liability," *ibid* at 549–50.

101 *Jones v Tsige*, 2012 ONCA 32 [*Jones*]. See also *Trout Point Lodge Ltd. v Handshoe*, 2012 NSSC 245 at para 55 [*Trout Point*] ("I am satisfied that in an appropriate case in Nova Scotia there can be an award for invasion of privacy or as the Ontario Court of Appeal called it, 'the intrusion upon seclusion'"); *Doucette v Nova Scotia*, 2016 NSSC 25 [*Doucette*]; *Capital District Health Authority v Murray*, 2017 NSCA 28 [*Murray*].

seclusion is one of four privacy-related tort claims identified by Professor William Prosser in his 1960 California Law Review article.[102]

Prosser reviewed the case law that had developed since Samuel Warren and Louis Brandeis first asserted the existence of a right to privacy that demanded legal recognition and access to legal remedies.[103] After reviewing over 300 cases decided by courts across the country, Prosser concluded that:

> What has emerged from the decisions is no simple matter. It is not one tort, but a complex of four. The law of privacy comprises four distinct kinds of invasion of four different interests of the plaintiff, which are tied together by the common name, but otherwise have almost nothing in common except that each represents an interference with the right of the plaintiff, in the phrase coined by Judge Cooley, 'to be let alone.' Without any attempt to exact definition, these four torts may be described as follows:
>
> 1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
> 2. Public disclosure of embarrassing private facts about the plaintiff.
> 3. Publicity which places the plaintiff in a false light in the public eye.
> 4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.
>
> It should be obvious at once that these four types of invasion may be subject, in some respects at least, to different rules.[104]

Of Prosser's list of privacy torts, the claim for intrusion upon seclusion is the one that is most relevant to respond to inappropriate access to health information. Of course, if the information is accessed *and* disclosed, the plaintiff could also make a claim for public disclosure of private facts about the plaintiff.

While Canadian courts have been receptive to the idea of privacy as an important value in the common law, they have historically shown some hesitation in recognizing privacy-specific tort claims.[105] The past decade has marked a shift in this attitude, with the courts beginning to acknowledge both the idea of privacy as an interest worth compensating, and the ever-increasing array of threats to privacy that are a feature of contemporary life. As observed by Justice Sharpe in *Jones v. Tsige*, sensitive personal information is now collected and stored in ways that render it exceedingly vulnerable to improper access.[106] As he explained, "[i]t is within the capacity of the common law to evolve to respond to the problem posed by the routine collection and aggregation of highly personal information that is readily accessible in electronic form."[107]

Justice Sharpe made these comments in the Ontario Court of Appeal's 2012 decision recognizing the claim for intrusion upon seclusion. The plaintiff made a claim for intrusion upon seclusion after learning that the defendant had, without authorization, accessed her

---

102 William L Prosser, "Privacy" (1960) 48:3 Cal L Rev 383.
103 Samuel D Warren & Louis D Brandeis, "The Right to Privacy" (1890) 4:5 Harv L Rev 193.
104 Prosser, *supra* note 102 at 389 [footnotes omitted].
105 See e.g. *Roth v Roth*, *supra* note 95; *Weingerl v Seo*, 2003 CanLII 13285 (ONSC) at paras 27–28.
106 *Jones*, *supra* note 101 at para 67.
107 *Ibid* at para 68.

bank records 174 times over a period of four years.[108] The plaintiff and defendant did not know one another, although both worked for the same bank, and the defendant was in a relationship with the plaintiff's ex-husband.[109] The Court held that the facts "[cried] out for a remedy,"[110] and concluded that the claim for intrusion upon seclusion is part of Ontario law. As the Court noted, this move was amply justified, based on the following considerations:

> The case law, while certainly far from conclusive, supports the existence of such a cause of action. Privacy has long been recognized as an important underlying and animating value of various traditional causes of action to protect personal and territorial privacy. *Charter* jurisprudence recognizes privacy as a fundamental value in our law and specifically identifies, as worthy of protection, a right to informational privacy that is distinct from personal and territorial privacy. The right to informational privacy closely tracks the same interest that would be protected by a cause of action for intrusion upon seclusion. Many legal scholars and writers who have considered the issue support recognition of a right of action for breach of privacy.[111]

As Justice Sharpe elaborated, the law's response to violations of privacy has evolved as new technologies have generated new threats to privacy interests.[112] And while some threats to privacy may be addressed by existing tort claims (including defamation, breach of confidence, and intentional infliction of mental distress),[113] it is often the case that one or more elements of these claims is not met by privacy-infringing conduct, leaving the plaintiff without a remedy unless the court is prepared to recognize a privacy-specific claim. The Nova Scotia Supreme Court recently commented on the need for privacy-specific claims for violations of privacy, explaining that "[m]odern life infringes on all aspects of personal privacy. Technology … has made it possible to track all aspects of a person's life … Existing causes of action, such as defamation … do not address the circumstances arising from the public disclosure of private facts."[114]

In the decade since the decision in *Jones*, courts in several Canadian jurisdictions have heard claims urging the adoption of the claim for intrusion upon seclusion.[115] In Nova Scotia, the argument appears to have been accepted, based on judicial commentary indicating that on the right set of facts, the Nova Scotia courts would be prepared to recognize the claim.[116] In some other Canadian jurisdictions, the courts have refused to strike out or dismiss claims for intrusion upon seclusion at early stages, suggesting that the courts are at least prepared

---

108 *Ibid* at para 2.
109 *Ibid*.
110 *Ibid* at para 69.
111 *Ibid* at para 66.
112 *Ibid* at para 67.
113 These claims are often raised together with claims for invasions of privacy, such as intrusion upon seclusion and public disclosure of private facts about the plaintiff. See e.g. *Jane Doe 72511 v Morgan*, 2018 ONSC 6607 [*Jane Doe #2*]; *Doe 464533 v D(N)*, 2016 ONSC 541 [*Jane Doe #1*]; *Shillington*, *supra* note 95.
114 *Racki v Racki*, 2021 NSSC 46 (recognizing the claim for public disclosure of private facts about the plaintiff in Nova Scotia).
115 See e.g. *Murray*, *supra* note 101; *Doucette*, *supra* note 101; *Hynes*, *supra* note 90; *Rancourt-Cairns v Saint Croix Printing and Publishing Company Ltd*, 2018 NBQB 19 [*Rancourt-Cairns*]; *Grant v Winnipeg Regional Health Authority*, 2015 MBCA 44 [*Grant*]; *Trout Point*, *supra* note 101; *Benison v McKinnon*, 2021 ABQB 843; *Al-Ghamdi v Alberta*, 2017 ABQB 684 [*Al-Ghamdi*], aff'd 2020 ABCA 81.
116 *Trout Point*, *ibid* at para 55; *Doucette, ibid*; *Murray*, *ibid*.

to hear and consider arguments in favour of recognizing the claim.[117] Recently, several jurisdictions have adopted the second tort in Prosser's list — the claim for "public disclosure of private facts about the plaintiff."[118] Only Ontario has recognized all four claims identified by Prosser,[119] and to date, Ontario is the only Canadian jurisdiction with case law explicitly accepting the claim for intrusion upon seclusion.[120]

This is slow progress. But there are reasons to be optimistic about the ongoing development of the common law on this front. Recently, we have seen more rapid and extensive action in terms of legal remedies for at least one type of privacy violation. The emergence of "revenge porn" (or non-consensual disclosure of intimate images) has been a catalyst for broader recognition of privacy interests as compensable interests. Unlike some privacy-related claims where there is disagreement about the urgency of the need for legal protection of privacy, or concern about the potential impact of protecting privacy on freedom of expression, there is widespread consensus that distributing or disclosing intimate images of a person without that person's consent should be prohibited by law.[121] Since 2015, eight provinces have passed legislation creating a tort claim for non-consensual disclosure of intimate images.[122] That same conduct is also subject to criminal sanction pursuant to amendments made to the *Criminal Code* in 2014.[123]

The Alberta Court of Queen's Bench recognized the claim for public disclosure of private facts about the plaintiff in 2021, in *ES v. Shillington*.[124] While the claim for intrusion upon seclusion is the more obvious fit for most inappropriate uses of health information, the decision in *Shillington* is considered here at some length as it indicates that the Alberta courts may be more open to recognizing tort privacy claims than they have been in the past.[125] As the claim was not defended, it is important to acknowledge that the facts that ground the decision in *Shillington* are based solely on the facts as alleged and testified to by the plaintiff.[126]

---

117 See e.g. *Hynes*, *supra* note 90; *Rancourt-Cairns*, *supra* note 115; *Grant*, *supra* note 115; *Tucci v Peoples Trust Company*, 2020 BCCA 246; *Severs v Hyp3R Inc*, 2021 BCSC 2261.

118 Note that most courts have not kept "embarrassing" in the name of the claim. See e,g. *Jane Doe #2*, *supra* note 113; *Jane Doe #1*, *supra* note 113; *Shillington*, *supra* note 95; *Racki v Racki*, *supra* note 114. Most of the cases recognizing this claim involve non-consensual disclosure of intimate images of the plaintiff, where we have also seen a swift legislative response in many Canadian jurisdictions.

119 Most recently, in *Yenovkian v Gulian*, 2019 ONSC 7279 at para 116 [*Yenovkian*], the Ontario Superior Court of Justice recognized the claim for "publicity which places the plaintiff in a false light in the public eye."

120 *Supra* note 101: the Nova Scotia courts have suggested that, on the right set of facts, the claim would be adopted there as well.

121 See e.g. Emily Laidlaw & Hilary Young, "Creating a Revenge Porn Tort for Canada" (2020) 96 SCLR (2d) 147 at para 6 [Laidlaw & Young, "Revenge Porn Tort"].

122 Manitoba (*Intimate Image Protection Act*, CCSM c I87); Alberta (*Protecting Victims of Non-Consensual Distribution of Intimate Images Act*, RSA 2017, c P-26.9 [*Intimate Images Act*]); Saskatchewan (*Sask Privacy Act*, *supra* note 87); Nova Scotia (*Intimate Images and Cyber-Protection Act*, SNS 2017, c 7); Newfoundland and Labrador (*Intimate Images Protection Act*, RSNL 2018, c I-22); Prince Edward Island (*Intimate Images Protection Act*, RSPEI 1988, c I-9.1) [*Intimate Images Act* PEI]; New Brunswick (*Intimate Images Unlawful Distribution Act*, SNB 2022, c1) [*Intimate Images Act* NB]; British Columbia (*Intimate Images Protection Act*, SBC 2023, c11) [*Intimate Images Act* BC].

123 *Criminal Code*, RSC 1985, c C-46, s 162.1 (as amended by *Protecting Canadians from Online Crime Act*, SC 2014, c 31).

124 *Shillington*, *supra* note 95.

125 See e.g. *Martin v General Teamsters, Local Union No 362*, 2011 ABQB 412 [*Martin*]; *Bank of Montreal v Cochrane*, 2010 ABQB 541 [*Cochrane*]. See also *Al-Ghamdi*, *supra* note 115.

126 *Shillington*, *supra* note 95 at para 7.

The plaintiff was the former romantic partner of the defendant and was physically and sexually assaulted by the defendant on multiple occasions. Over the course of her relationship with the defendant, the plaintiff had shared intimate photographs of herself with him. The photographs were provided by the plaintiff on the understanding that the photographs were for the defendant alone and would not be shared or distributed.[127]

Toward the end of the relationship, the defendant told the plaintiff that he had posted the intimate photographs of her online. The plaintiff was able to locate some of the images, including on pornography sites.[128] The defendant told the plaintiff that he had posted images in 2006, and she was also able to locate images posted in 2018.[129] In early 2021, the plaintiff was still able to find some of her images online.[130]

The effect on the plaintiff of these images having been posted online has been significant. The plaintiff was recognized by a neighbour who saw images of her online and who made comments of a sexual nature.[131] As described by Justice Inglis, the plaintiff "suffers nervous shock, psychological and emotional suffering, depression, anxiety, sleep disturbances, embarrassment, humiliation, and other impacts to her wellbeing."[132] Since the relationship ended in late 2016, (after the plaintiff was violently sexually and physically assaulted by the defendant and fled the relationship with her children),[133] she has been in treatment to try to overcome the harmful effects of her relationship with the defendant.[134]

The plaintiff's claim asked the Court of Queen's Bench to recognize "public disclosure of private facts" as a valid tort claim in Alberta and sought damages for the public disclosure of the intimate images posted by the defendant. She also sought damages for breach of confidence, assault, sexual assault, battery, and intentional infliction of mental distress.[135] The plaintiff was awarded damages for all of the claims she raised.

With respect to the public disclosure of private facts claim, Justice Inglis began by articulating the test for the recognition of a new tort claim, as set out by the Supreme Court of Canada in *Nevsun Resources Ltd. v. Araya*.[136] In short, the test requires that the new tort "must reflect a wrong, be necessary to address that wrong, and be an appropriate subject of judicial consideration."[137]

Justice Inglis noted that the decision of the Ontario Court of Appeal in *Jones*, recognizing the tort for intrusion upon seclusion, was cited with approval by the Supreme Court of Canada in *Nevsun*.[138] In considering the plaintiff's argument, she cited the Ontario case law recognizing both intrusion upon seclusion[139] and public disclosure of private facts about the

127 *Ibid*.
128 *Ibid* at para 11.
129 *Ibid*.
130 *Ibid*.
131 *Ibid.*
132 *Ibid* at para 12.
133 *Ibid* at para 15.
134 *Ibid*.
135 *Ibid* at para 2.
136 *Nevsun Resources Ltd v Araya,* 2020 SCC 5 [*Nevsun*].
137 *Ibid* at para 237.
138 *Shillington*, *supra* note 95 at para 25.
139 *Jones*, *supra* note 101.

plaintiff.[140] Both torts are (as noted above) derived from the list of four privacy-related claims identified by Prosser.[141]

All of the Ontario cases reviewed by Justice Inglis pointed out that privacy has long been acknowledged as a key legal value deserving protection.[142] All also noted the profound threats to privacy that are a product of evolving technology.[143] In each case the Ontario courts concluded that a legal response to invasions of privacy is needed in at least some circumstances. In one of the cases, *Jane Doe #2*, the defendant had posted sexually explicit images of the plaintiff without her knowledge or consent. The trial judge in that case commented on the decision in *Jones* and its recognition of a new privacy-related claim and said that she could "see no reason why this protection should not extend to prevent the unauthorized publication of intimate images, given the privacy rights at stake and the serious harm caused by such publication."[144]

After considering a number of other cases in which privacy-related claims have been accepted by Canadian courts,[145] Justice Inglis turned to an application of the principles from *Nevsun*. She concluded that recognition of the claim is necessary to address the wrong in question, as it is not fully addressed by any existing remedy.[146] While Alberta has legislation dealing with non-consensual disclosure of intimate images,[147] the legislation was not in force at the time of the defendant's conduct or when the plaintiff learned about his conduct, and therefore did not provide a foundation for the plaintiff's claim.[148] In addition, the statutory scheme created by the *Intimate Images Act* provides a claim in narrowly defined circumstances: the only conduct prohibited by the statute is the distribution of intimate images (and not, for example, personal or private information that is not sexual in nature or that is not captured in the form of images); the statute also narrowly defines intimate images to include images where the "victim is nude, exposing their genital or anal regions or breasts, or is engaged in sexual activity."[149] Moreover, the *Intimate Images Act* does not prohibit private sharing of intimate images.[150]

Justice Inglis then turned to the existing tort claims that arise in circumstances like those in this case, including intentional infliction of mental distress and breach of confidence, concluding that both entail elements that could prove to be barriers to recovery for some claimants. In the case of breach of confidence, the plaintiff must demonstrate that the image they shared with the defendant was confidential and that it was "communicated in confidence."[151] Where a defendant has acquired the images without agreeing to their

---

140 *Jane Doe #2*, *supra* note 113; *Jane Doe #1*, *supra* note 113. *Jane Doe #1* was a default judgment and was subsequently set aside at the request of the defendant.

141 Prosser, *supra* note 102.

142 *Jones*, *supra* note 101 at para 66; *Jane Doe #2*, *supra* note 113 at para 87 (noting that privacy is an important *Charter* value); *Jane Doe #1*, *supra* note 113 at paras 35–40 (agreeing with the reasoning in *Jones*, *ibid*).

143 *Jones*, *ibid*; *Jane Doe #1*, *ibid*; *Jane Doe #2*, *ibid*.

144 *Jane Doe #2*, *ibid* at para 96.

145 *Shillington*, *supra* note 95 at paras 23–33.

146 *Ibid* at para 34.

147 *Intimate Images Act*, *supra* note 122.

148 *Shillington*, *supra* note 95 at para 41.

149 *Ibid* at para 42; *Intimate Images Act*, *supra* note 122, s 1(b).

150 *Shillington*, *ibid*.

151 *Ibid* at para 44.

confidentiality,[152] or where the defendant is the party who captures or generates the images, a claim for breach of confidence could not succeed. The claim for intentional infliction of mental distress includes a requirement to prove that the defendant's conduct was "calculated to produce harm" and that it resulted in a "visible and provable illness."[153] Both of these requirements could pose challenges for plaintiffs in some instances, particularly the latter where the plaintiff must demonstrate "psychological disturbance … [that is] … serious and prolonged and rise[s] above the ordinary annoyances, anxieties and fears that people living in society routinely, if sometimes reluctantly, accept."[154]

Justice Inglis quickly dispensed with the requirement from *Nevsun* that the tort claim proposed must be a response to a wrongdoing, noting that privacy is a fundamental legal value, and that technology currently poses an extreme threat to privacy given the ease with which private information can be accessed and disseminated. Finally, Justice Inglis concluded that the claim raised by the plaintiff is appropriate for judicial adjudication. Here, she referred to case law as well as provincial legislation and a provision of the *Criminal Code* protecting victims of non-consensual disclosures of intimate images. As she explained, "[w]hen conduct attracts legislative and parliamentary attention, its wrongfulness is apparent."[155]

The claim for public disclosure of private facts is now part of Alberta law, based on the following elements:

(a) the defendant publicized an aspect of the plaintiff's private life;

(b) the plaintiff did not consent to the publication;

(c) the matter publicized or its publication would be highly offensive to a reasonable person in the position of the plaintiff; and,

(d) the publication was not of legitimate concern to the public.[156]

The case law outlined above represents significant progress in the sense of expanding legal protection for privacy interests, if not specifically in the context of health information privacy. It also signifies that Canadian courts are attentive to the need for remedies for privacy violations, and that they are prepared to offer those remedies in appropriate circumstances. While a claim for intrusion upon seclusion is a more obvious fit for unauthorized access to health records, the public disclosure of private facts claim as recognized in *Shillington* is important to consider here, because it provides a common law remedy for the disclosure of private information without consent and where there is no legitimate public interest in the information. Health information is an "aspect of the plaintiff's private life" and its non-consensual publication would be "highly offensive to a

---

152 *Ibid* at para 46.
153 *Ibid* at para 47, citing *Rahemtulla v Vanfed Credit Union* (1984), 51 BCLR 200 (Sup Ct).
154 *Mustapha*, *supra* note 97 at para 9.
155 *Shillington*, *supra* note 95 at para 62.
156 *Ibid* at para 68. The test articulated by Justice Inglis qualifies the "highly offensive" requirement a bit differently than prior Canadian case law, in that the plaintiff must show that the matter publicized or its publication would be highly offensive to a reasonable person in the position of the plaintiff.

reasonable person."[157] That said, as I explain in more detail below, it is becoming increasingly clear that allowing the common law to continue to evolve incrementally leaves a great deal to chance, and may not, in the end, result in an adequate legal response to invasions of privacy.

IV. NARROWING ALBERTA'S PRIVACY ACCOUNTABILITY GAPS

Finding legal solutions that will permit us to respond meaningfully to violations of privacy is undeniably a challenge. Privacy is an imprecise concept that encompasses a multitude of ideas, and can shift depending on time and context.[158] Privacy also overlaps conceptually with other interests that are already protected to some extent by the law.[159] It is an idea that changes over time as people become accustomed to their information being accessed and used in different ways. In 2012, many of us found it shocking to see targeted online ads on web browsers that were related to our recent internet searches. In the decade since then, concerns about how to protect privacy have continued to grow as technology has enabled new and more efficient ways to invade privacy.[160] But even if we cannot readily identify a way to perfectly safeguard privacy, or an ideal way to respond to privacy breaches, we can absolutely improve on existing safeguards by closing (or at least narrowing) some of the troubling gaps in accountability. At a minimum, we can take steps to enhance access to remedies for invasions of privacy specifically in the health information context.

As Justice Inglis' reasons in *Shillington* make clear, it is essential to afford remedies for privacy violations via both legislative and common law routes. The claim in *Shillington* was based on conduct by the defendant that pre-dated the Alberta legislation addressing non-consensual disclosure of intimate images.[161] Accordingly, the plaintiff could not pursue a claim based on the tort created by the *Act*, and recognition of the claim for public disclosure of private facts was required in order to provide the victim with a remedy. Justice Inglis also noted that the *Intimate Images Act* only provides a remedy for non-consensual disclosure of intimate images, not for intimate information more broadly, while the common law claim is available to address a wider range of privacy-infringing conduct.

The most straightforward way to begin to address the current gap in accountability is through legislative change. Most Canadian jurisdictions have health information statutes in place, but, as explained earlier, only Ontario's health information law includes a private right of action that can be used to seek damages for a breach of the statute.[162] In my view, the absence of a private remedy is a significant gap in legal protection for health information privacy. Arguably, it means that one of the major objectives of Alberta's *HIA* — "to establish strong and effective mechanisms to protect the privacy of individuals with respect to their health information and to protect the confidentiality of that information"— is not being fully

---

157 *Ibid* at para 65, quoting *Jane Doe #2*, *supra* note 113 at para 99.

158 See e.g. Elizabeth Paton-Simpson, "Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places" (2000) 50 UTLJ 305 at 308–309; Warren & Brandeis, *supra* note 103; WA Parent, "A New Definition of Privacy for the Law" (1983) 2:3 Law & Phil 305 at 306–307.

159 See e.g. *Jones*, *supra* note 101; *Roth v Roth*, *supra* note 95.

160 *Jones*, *ibid* at para 67; *Jane Doe #2*, *supra* note 113 at paras 93–94.

161 *Intimate Images Act*, *supra* note 122.

162 *PHIPA* ON, *supra* note 65, s 65.

achieved.[163] A complainant whose health information has been accessed inappropriately may be satisfied by the conviction of the wrongdoer, but no damages will be available to the person for harm they suffer as a result of the unlawful use of their health information. If the inappropriate access is by a health care provider, a complaint may be made to the relevant regulatory body. This may result in discipline, but again will not provide any remedy for the individual whose records have been used or disclosed in a manner that contravenes the *HIA*. And even with the possibility of conviction or discipline, there will be situations in which there are no consequences for violating privacy. In the South Campus Health incident described earlier, few of the 49 employees who invaded the privacy Christine Hagan faced any consequences for their actions. Absent the ability to pursue a claim for compensation against the individual providers or AHS (the custodian with ultimate responsibility for the collection, use and disclosure of the health information), it appears that no one — individual or organization — has been made accountable for this egregious violation of privacy.

An amendment adding a private right of action would be a useful addition to the *HIA*, as it would permit the victim of unauthorized access to seek compensation from both the individual wrongdoer and potentially also the organizational custodian. I would favour a less restrictive approach than that employed in Ontario's *PHIPA* (where the private right of action is contingent on either a conviction or a final order of the privacy commissioner, and where damages are limited to "actual harm"),[164] but even with those constraints, adding a private right of action would be a step in the right direction.[165]

In addition to advocating in favour of a legislative amendment, I would urge plaintiffs and their lawyers to pursue the claim for intrusion upon seclusion in the Alberta courts. Based on the reasoning in *Shillington*,[166] the Alberta courts now appear to be receptive to the recognition of tort claims related to invasions of privacy in appropriate circumstances. All of Justice Inglis' observations about the necessity and wisdom of recognizing the tort claim for public disclosure of private facts about the plaintiff are equally applicable to the claim for intrusion upon seclusion, excepting the fact that there is legislation in place aimed at the same concerns. While there is some older case law that seems to suggest that Alberta law does not include a claim for invasion of privacy, those cases do not analyze the issues clearly or sufficiently and should not be taken as authority for the conclusion that the door to such claims is closed.[167]

While Justice Sharpe made it clear in *Jones* that not all intrusions into personal information will satisfy the requirements of the intrusion upon seclusion claim, intentional snooping into health records along the lines of the examples provided above would almost certainly be found to meet all of the elements of the claim: it is intentional conduct that

---

163 *Ibid*, s 2(a).

164 *Ibid*, s 65(3).

165 *Ibid*. It is worth noting here that section 65 of the *PHIPA* ON has had little judicial consideration in reported case law, so it is difficult to say with certainty how effective such a provision might be in Alberta. Given that Ontario also recognizes the tort of intrusion upon seclusion (the application of which is not precluded by the statutory provision: *Hopkins v Kay*, 2015 ONCA 112), the statutory private remedy may not be relied on by plaintiffs.

166 *Shillington*, *supra* note 95.

167 *Martin*, *supra* note 125; *Cochrane*, *supra* note 125; *Al-Ghamdi*, *supra* note 115.

intrudes upon the plaintiff's private affairs without lawful justification, and is conduct that would be highly offensive to a reasonable person.[168] As Justice Sharpe explained:

> A claim for intrusion upon seclusion will arise only for deliberate and significant invasions of personal privacy. Claims from individuals who are sensitive or unusually concerned about their privacy are excluded: it is only intrusions into matters such as one's financial or health records, sexual practices and orientation, employment, diary or private correspondence that, viewed objectively on the reasonable person standard, can be described as highly offensive.[169]

Should the courts adopt a test similar to that accepted by Justice Inglis in relation to the public disclosure of private facts claim, (that the intrusion is highly offensive to a person *in the position of the plaintiff*),[170] this element would be even more likely to be satisfied in cases involving unauthorized access to health information.

Recognition of the claim for intrusion upon seclusion would also permit the possibility that public bodies can be liable for violations of health information privacy (as well as violations of privacy more generally), either directly or vicariously (as the employer of the tortfeasor). This would be an improvement over the current state of affairs, although not without limitations. The strict requirements of the claim for intrusion upon seclusion may make it a challenge for victims to make successful direct claims against institutions and organizations. In an intrusion upon seclusion claim, the claimant must show that the defendant invaded their privacy through intentional or reckless conduct. This might be difficult to prove against a public body where, for example, the intrusion results from a failure to implement adequate safeguards to ensure that data is secure against access by those outside the organization.[171] Similarly, intention or recklessness may be difficult to prove if the organization's conduct is a failure to track the safeguards that are in place, as is frequently the case in instances of snooping into health records. In such circumstances, it will be difficult to establish intentional invasion of privacy by the defendant.[172]

Seeking to have an organizational custodian found vicariously liable might be a more effective strategy. Employers can be vicariously liable for torts committed by employees — including intentional torts — where the court agrees that there is a "strong connection" between the opportunity for wrongdoing created by the employer's enterprise and the conduct engaged in by the employee.[173] Vicarious liability is available where the defendant employee has committed a tort in the course of employment.[174] Many instances of unauthorized access to health information seem to involve individuals (either custodians or

---

168 A recent Ontario decision makes it clear that not all instances of unauthorized access to health information will be considered "highly offensive." In *Stewart v Demme*, 2022 ONSC 1790 (Div Ct) at para 3, the Divisional Court overturned the certification of a class action of a claim for intrusion upon seclusion. The claim arose out of the theft of thousands of Percocet pills by a nurse working in the William Osler Hospital. In order to disguise her conduct, the defendant viewed health information belonging to thousands of patients. The Divisional Court held that the defendant's conduct did not meet the threshold of being "highly offensive to a reasonable person," as the access to information was "limited and the access was fleeting and incidental to the medication theft."

169 *Jones*, *supra* note 101 at para 72.

170 *Shillington*, *supra* note 95 at para 68.

171 von Tigerstrom, "Direct and Vicarious Liability," *supra* note 96 at 555–56.

172 *Ibid*.

173 *Bazley v Curry*, [1999] 2 SCR 534 at 560.

174 *Ibid* at 541.

affiliates) with employment-based access to records using that access in an inappropriate way, such as to look up the health information of friends, family, or acquaintances, or to satisfy their curiosity about a patient in whose care they are not involved. It is certainly arguable that the threat of vicarious liability for organizational custodians would incentivize both the adoption of the most intensive safeguards available, and careful oversight of existing safeguards.[175] In Alberta at present, there is no possibility of vicarious liability because there is no tort claim that can readily be pursued against someone who misuses their authority to access health information. In my view, this provides yet another argument to encourage the recognition of a tort claim (either by statute or the common law) to provide health information custodians with the strongest motivation to preserve the security of health information.

As is clear from the foregoing discussion, both a statutory right of action and the intrusion upon seclusion claim, while improvements on the current state of the law in Alberta, have limits. One such limit is the common law process itself. The possibility of change depends on the existence of a claimant with an appropriate set of facts and the time, energy, and financial resources to pursue their claim to trial. As access to justice becomes increasingly challenging,[176] this combination becomes more and more elusive. In the context of privacy claims in particular, it is perhaps made even less likely given the current approach to damages awards in the intrusion upon seclusion claim. The tort is actionable without proof of harm, but in the absence of actual loss, damages will generally be "modest."[177]

It is difficult to feel confident that claimants — particularly those seeking to have the court recognize a new tort claim — will continue to see much utility in seeking relief via the common law given the uncertainty of success in court and with enforcement, coupled with the prospect of only modest damages. This does not mean that there is no value in continuing to pursue common law remedies, it is simply an acknowledgement that leaving individual claimants to do all of the heavy lifting might not lead to significant improvements in privacy protection, at least in the short term.

In addition to the suggestions made above, there is more we can do to meaningfully protect privacy interests in Alberta — both in the health information context and in general. Progress in responding to invasions of privacy generally will also improve on the law's ability to respond to access to health information in contravention of the *HIA*, and so it is useful to briefly consider the larger picture. A major question is whether to stay focused on the Prosser-style torts that take a fairly constrained approach to privacy, or instead move toward recognition of a more general tort claim for invasion of privacy.

Although not terribly old in view of the timeline of the common law itself, the privacy-related torts that play a major role in Canadian law were identified by Prosser more than 60

---

175 von Tigerstrom, *Information & Privacy Law*, *supra* note 44 at 484.

176 It has long been recognized that access to justice is a significant problem in Canada. See e.g. Trevor CW Farrow, "What Is Access to Justice?" (2014) 51:3 Osgoode Hall LJ 957 at 962–63; Trevor CW Farrow & Lesley A Jacobs, eds, *The Justice Crisis: The Cost and Value of Accessing Law* (Vancouver: UBC Press, 2020).

177 *Jones*, *supra* note 101 at para 87. As Justice Sharpe explained: "In my view, damages for intrusion upon seclusion in cases where the plaintiff has suffered no pecuniary loss should be modest but sufficient to mark the wrong that has been done. I would fix the range at up to $20,000."

years ago.[178] Prosser's classification scheme for privacy-related torts has been influential in the evolution of the American and Canadian common law around privacy.[179] Indeed, "[i]t is impossible to talk about privacy in American tort law without considering William Prosser."[180] And, as has been noted by some scholars, the focus on Prosser's understanding of privacy-related tort claims has had both positive and negative effects on the law's development.[181] While Prosser's work gave "tort privacy order and legitimacy, he also stunted its development in ways that have limited its ability to adapt to the problems of the Information Age."[182]

As these privacy torts continue to evolve in Canadian jurisdictions, it is worth asking whether — even if the courts are prepared to recognize more such claims — judicial recognition of these distinct privacy-related claims will lead to meaningful protection of privacy now and into the future. As Emily Laidlaw has explained, much has changed in the past 60 years, including both our ideas about privacy and the methods available to invade it. In her view, it is time to consider a new approach, in place of one that she describes as being "ossified." As she explains:

> What was ossified? Among other things, the belief that privacy is what happens when we are secluded or alone, that privacy only protects deviant or intimate behaviour, and that context does not matter. In the age of technology, our privacy is vulnerable by our act of existing, because we cannot avoid going outside, using technology, sharing our personal information or otherwise being exposed. Many things we might think of as privacy invasions, such as deepfakes, catfishing, some forms of doxing, and amplification of content through search engines, would likely not be actionable as a privacy tort. The torts are also difficult to square with *Charter* jurisprudence on privacy, particularly the contextual factors courts considered in assessing a reasonable expectation of privacy and balancing competing rights.[183]

Given contemporary understandings of privacy and the ever-increasing array of tools available to invade it, several scholars (including Laidlaw) have suggested that specific tort claims like those identified by Prosser are not the best way forward.[184] In favour of relying on the specific categories of privacy identified by Prosser, some of these scholars propose a general tort claim for invasion of privacy (such as the statutory claim discussed above)[185] based on whether the claimant has a reasonable expectation of privacy in the circumstances. Each of the torts identified by Prosser has specific elements: intrusion upon seclusion requires that the defendant intrude into the plaintiff's solitude or seclusion, suggesting that

---

178 Prosser, *supra* note 102.

179 Neil M Richards & Daniel J Solove, "Prosser's Privacy Law: A Mixed Legacy" (2010) 98:6 Cal L Rev 1887. Prosser's classification scheme is invariably discussed by courts contemplating recognition of a new privacy-related tort. *Jones*, *supra* note 101; *Shillington*, *supra* note 95; *Jane Doe #2*, *supra* note 113; *Jane Doe #1*, *supra* note 113; *Yenovkian*, *supra* note 119.

180 Richards & Solove, *ibid* at 1888.

181 *Ibid* at 1889. See also Danielle Keats Citron, "Mainstreaming Privacy Torts" (2010) 98 Cal L Rev 1805 at 1824–31.

182 Richards & Solove, *ibid* at 1890.

183 Emily Laidlaw, "The Future of the Tort of Privacy: Is Alberta's Lag its Opportunity to Lead?" *CBA National Magazine* (30 March 2021), online: [perma.cc/S5AJ-2NQ3] [Laidlaw, "Future of Tort"], commenting on why the torts identified by Prosser in 1960 are not our best bet for the future of protecting privacy, particularly in an era of technological invasions of privacy.

184 Laidlaw, "Future of Tort," *ibid*. See also Hunt, "Reasonable Expectations," *supra* note 91; Hunt & Shirazian, "Statutory Privacy Torts," *supra* note 89.

185 *Privacy Act* BC, *supra* note 87, s 1(1); *Privacy Act* Sask, *supra* note 87, s 2; *Privacy Act* Man, *supra* note 87, s 2(1); *Privacy Act* NL, *supra* note 87, s 3(1).

the claim is not available if the claimant's privacy is invaded in a more public context.[186] The claim also requires that intrusion is intentional or reckless, and that the invasion "would be highly offensive to a reasonable person."[187] In place of these specific and variable elements, the claim for invasion of privacy would assess whether the claim has merit based on whether the claimant had a reasonable expectation of privacy in the circumstances. The idea advanced by Chris Hunt is that the "reasonable expectation" inquiry would serve two purposes: it would answer the threshold question of whether there was an invasion of privacy at all, as well as the question of whether the invasion is such that some sort of legal response is appropriate.[188]

An approach grounded in the question of the claimant's reasonable expectation of privacy has a number of potential advantages over the adoption of several distinct privacy-related torts, each with their own set of requirements. The idea of a reasonable expectation of privacy is a familiar legal concept that plays a central role in assessing whether the *Charter* right to be free from unreasonable search and seizure has been violated.[189] It also streamlines the analysis of conduct that could form the basis for more than one of the Prosser-style tort claims, such as intrusion upon seclusion and publication of private facts about the plaintiff. Chris Hunt and Nikta Shirazian have pointed out that a person who secretly captures private images of the plaintiff and publishes those images has committed both of the above-mentioned torts.[190] But the elements of the torts are not in complete alignment. Intrusion upon seclusion requires proof that the defendant's conduct was intentional or reckless, but there is no 'intent' requirement for publication of private facts.[191] The authors worry that these distinctions could lead to inconsistent development of these tort claims, even though some claims that encompass both torts could be based on a single series of actions by the defendant.[192] In any case, it does seem a bit strange to imagine breaking down an invasion of privacy into its component parts in order to be able to offer a remedy to the claimant, rather than simply acknowledging that, as a whole, the defendant's conduct amounts to an invasion of privacy.

This idea is not universally accepted. Legal scholars Samuel Beswick and William Fotherby have argued that a more comprehensive tort claim for invasion of privacy based on whether the claimant had a reasonable expectation of privacy is not necessary in the Canadian jurisprudential context.[193] They note that the scholars advocating this approach suggest that other Commonwealth jurisdictions should adopt the approach that has been taken in England and Wales. Beswick and Fotherby assert that such calls miss some key

---

186 See e.g. Paton-Simpson, *supra* note 158; Hunt, "Reasonable Expectations," *supra* note 91.

187 *Shillington*, *supra* note 95 at para 68; *Jones*, *supra* note 101 (this is also required for the public disclosure of private facts claim, although as noted earlier, the Alberta Court of Queen's Bench modified this requirement in *Shillington* so that the question of whether the publication of the information (or the matter publicized) would be highly offensive is specific to a reasonable person in the position of the plaintiff).

188 Hunt & Shirazian, "Statutory Privacy Torts," *supra* note 89 at 16–17.

189 Hunt, "Reasonable Expectations," *supra* note 91 at para 7; *Hunter v Southam Inc*, [1984] 2 SCR 145 at 167–68; *R v Dyment*, [1988] 2 SCR 417 at para 15.

190 Hunt & Shirazian, "Statutory Privacy Torts," *supra* note 89 at 4.

191 *Ibid*. Although it is worth noting that posting intimate images of someone to a website, or sharing private information with others, is most often likely to be intentional (apart from circumstances where an email is inadvertently sent to the incorrect recipient).

192 *Ibid*.

193 Samuel Beswick & William Fotherby, "The Divergent Paths of Commonwealth Privacy Torts" (2018) 84 SCLR (2d) 225.

considerations. In particular, the uniquely brazen and aggressive tabloid culture in England is meaningfully different from the media culture in other Commonwealth jurisdictions.[194] In addition, the English courts have proceeded to develop the common law in a manner that comports with the *Human Rights Act, 1998*.[195] The *Human Rights Act* incorporates the rights protected in the European Convention on Human Rights into domestic law.[196] Article 8 of the ECHR explicitly recognizes a right to "respect for private and family life."[197] The result is the evolution of the common law of privacy with a "human rights orientation."[198] The authors suggest that privacy torts with a "restrained scope" (such as the distinct privacy-related torts based on Prosser's list) are sufficient to safeguard privacy interests.[199] Others have noted that using the claimant's reasonable expectation of privacy as the touchstone to determine whether or not privacy has been invaded is potentially problematic, in that it is a concept prone to attrition as we become increasingly accustomed to privacy infringements. In other words, the danger with a focus on the reasonable expectation of the plaintiff is that "once an intrusive practice becomes sufficiently widespread … (be it videoing people in ambulances, bugging Narcotics Anonymous meetings, or spying on people in public toilets) then claimants will have no action for breach of privacy if it occurs."[200]

I agree with Laidlaw, Hunt, and other scholars that in the long run, a general claim aimed at remedying invasions of privacy is a more useful and appropriate response than continuing to follow the path identified by Prosser in 1960. Requiring plaintiffs to demonstrate intentional conduct, and to show that the defendant's conduct was objectively "highly offensive" may well frustrate many claims. By contrast, a claim based on invasion of privacy more generally would be available to address diverse forms of privacy-infringing conduct, unconstrained by the need to demonstrate the rigid elements of claims like intrusion upon seclusion. But given the current situation in Alberta, where there is no statutory tort protecting privacy, no private right of action for violations of health information privacy or where a public body is the potential defendant, and no recognition of the claim for intrusion upon seclusion, any move in the direction of increased access to legal recourse for invasions of privacy would be a substantial improvement.[201]

In addition to the approaches outlined above, other creative approaches have been proposed to protect privacy rights in specific contexts. In the context of non-consensual disclosure of intimate images, we have seen more rapid reform of privacy law than has been typical. In part, this may be a result of general agreement respecting the importance of

---

194 *Ibid* at paras 54–55.

195 *Human Rights Act 1998* (UK), c 42; Beswick & Fotherby, *supra* note 193 at paras 13–16.

196 Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953) [ECHR].

197 *Ibid*, art 8.

198 Beswick & Fotherby, *supra* note 193 at para 15.

199 *Ibid* at paras 72–74.

200 Nicole A Moreham, "Privacy in the Common Law" (2005) 121 LQR 628 at 647. Moreham suggests that this concern should encourage a shift away from a focus on a claimant's expectation of privacy to their "desire" for privacy. Daniel J Solove, "Conceptualizing Privacy" (2002) 90:4 Cal L Rev 1087 at 1142. Solove explains this objection: "If we focus simply on people's current expectations of privacy, our conception of privacy would continually shrink given the increasing surveillance in the modern world. Similarly, the government could gradually condition people to accept wiretapping or other privacy incursions, thus altering society's expectations of privacy." Solove's response to this concern is that there is a normative component to privacy, in addition to empirical and historical components.

201 This is also the case in a few other Canadian jurisdictions, including New Brunswick, Prince Edward Island, and the territories.

prohibiting such conduct, and recognition of the harm it can cause. Arguably the high level of consensus about the egregious nature of this conduct has led courts to move more quickly to recognize the claim for public disclosure of private facts about the plaintiff than some of the other privacy-specific claims. It is likely that there is a similarly high level of agreement respecting the importance of protecting the privacy of health information, so it is worth considering whether there are useful lessons that we can draw from the treatment of intimate images in privacy law.

In order to permit the law to continue to be appropriately responsive to the wishes of victims of non-consensual distribution of intimate images, the Uniform Law Conference of Canada (ULCC) has recommended an innovative approach to legislation aimed at combatting revenge porn. Based on a report by Hilary Young and Emily Laidlaw,[202] the ULCC has proposed model legislation that creates a process by which victims can quickly obtain what they most desire: "the destruction, removal or de-indexing of the intimate image as cheaply and quickly as possible."[203] To date, New Brunswick has adopted legislation based on the ULCC's proposal, and Prince Edward Island and British Columbia have adopted a very similar statute.[204]

The *Uniform Act* creates two distinct tort claims — one is a traditional fault-based claim for damages.[205] The other claim provides a way for victims to seek declaratory relief (and potentially nominal damages as well). It also permits the court to order the defendant to "make every reasonable effort" to take down or otherwise "make the … image unavailable to others."[206] Importantly, this second claim is based on strict liability rather than fault; all that the plaintiff must prove in order to obtain relief under this section is that "the image is an intimate image of the applicant, and [that] the respondent distributed the intimate image."[207]

A strict liability approach such as the one proposed by the Uniform Act seems unobjectionable in circumstances where intimate and, in some cases graphic, images of a claimant are made available to the world at large without the claimant's consent. Strict liability is the exception in our fault-based tort system and is likely not appropriate in all types of privacy invasions.[208] But it is nevertheless worth highlighting as an example of a

---

202 Laidlaw & Young, "Revenge Porn Tort," *supra* note 121.

203 Uniform Law Conference of Canada, "Uniform Non-Consensual Distribution of Intimate Images Act (2021)" (2021) at 1, online (pdf): [perma.cc/3K8P-KSCU] [Uniform Act].

204 *Intimate Images Act* PEI, *supra* note 122; *Intimate Images Act* NB, *supra* note 122; *Intimate Images Act* BC, *supra* note 122.

205 Uniform Act, *supra* note 203, s 5(1)(f).

206 *Ibid*, s 4(2)(d) (the section also permits the court to grant an order requiring reasonable efforts on the part of the intermediary, person, or organization to remove or de-index the image, and make any other order that the court considers "just and reasonable in the circumstances."

207 *Ibid*, ss 4(2)(a)–(b). Danielle Keats Citron, "Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age" (2007) 80:2 S Cal L Rev 241 at 265–66. Strict liability has also been raised by American privacy scholar Danielle Citron. Citron has made the argument that digital databases represent a risk in today's world like water reservoirs did at the beginning of the Industrial Age. She explains that there is no degree of reasonable conduct that can completely prevent access to sensitive information in digital databases, meaning that negligence law will not be able to respond effectively to theft of sensitive information by a third party. She refers to digital databases (or "cyber-reservoirs") as "ultrahazardous activities — those with significant social utility and significant risk" and suggests that the appropriate legal response is to impose strict liability in order to reduce the level of activity in this area by requiring database operators to "internalize the full costs of their activities."

208 See e.g. Allen M Linden & Bruce Feldthusen, *Canadian Tort Law*, 9th ed (Toronto: LexisNexis Canada, 2011) at 539–40.

creative approach to finding solutions that focus on providing the remedy best suited to specific instances of privacy-invading conduct.

V. CONCLUSION

In spite of having three separate pieces of information and privacy legislation on the books, Alberta's privacy regime does not offer sufficient protection for privacy. While statutes that limit how personal information — including health information — can be collected, used, and disclosed are key pieces of a rigorous privacy regime, they provide only a partial response to the need for privacy protection. As reliance on EHRs and other electronic forms of information storage increases, the need for strong protection for privacy is now more pressing than ever.

Changes to both legislation and the common law are needed in order for Alberta to get closer to a comprehensive regime for protecting privacy. The good news is that there are some straightforward steps that can be taken to shore up legal protections for health information privacy. The *HIA* could be amended to add a private right of action for breaches of the statute. In addition, the courts can be pressed to recognize the tort claim for intrusion upon seclusion. It has been encouraging to see some progress in the Canadian common law around privacy, beginning in 2012 with the Ontario Court of Appeal's decision in *Jones*. But that decision is now more than a decade old, and the claim remains unavailable in Alberta. In any case, while these steps would mark a vast improvement over the current state of the law, they will only take us part of the way toward a meaningful legal response to privacy infringements. Ultimately, we need to take a more complete and creative approach to legal protection of privacy interests in order to respond effectively to current and future threats to privacy.

[*this page is intentionally blank*]