THE LITIGATION CONSEQUENCES OF CYBERSECURITY BREACHES – PART I

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

Table of Contents

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

Introduction

Cybercriminals are on the loose, and civil litigators – many others, too – must be ready to help remedy the consequences.

The authors of this article, litigators all, propose to address the risks cybersecurity breaches pose and the civil remedies that do or may present themselves as appropriate.

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

Given these nascent states, our vista is limited. Just as there is no perfect technology or perfect technological solution to cyberbreaches, civil litigation as yet offers no single or perfect solution to cybersecurity issues.[1] Cyberbreach litigation is only beginning to take shape. Its *Donoghue v Stevenson* moment has yet to arrive.

It is in that context that we approach our inquiry. It will fall into two parts. Part 1 will address (i) cybersecurity terms and concepts, and (ii) the statutory Canadian framework for data security and privacy. Part 2, to be released in March 2023, will focus on (i) common law remedies, and (ii) some liability avoidance strategies.

Part 1: Cybersecurity and Canadian Legislation

Lest anyone doubt that cybersecurity is a burning issue in Canada, they need only Google (securely, of course)[2] "cybersecurity

1. Bryan P Schwartz et al, "Cybersecurity and Law Firms", *Asper Review of International Business and Trade Law*, Introduction, Volume 21 Special Edition – 2021, CanLIIDocs 988, https://canlii.ca/t/t58s, accessed November 24, 2022.
2. A host of search engines purport to offer Internet searching without collecting personal information, in contrast with the most popular search engines – Google and Bing, for example – that do collect data. These privacy-oriented search engines include duckduckgo, startpage and qwant.

Canada". In 0.63 seconds, the oracle of online omniscience returns 156 million results. That number drops to 51.5 million results if one limits the search scope to the past year.

Clearly, Canada is searching for answers about cybersecurity. And rightly so. Security breaches are proliferating in Canada.

In June 2022 alone, the Canadian Centre for Cyber Security[3] issued 70 cybersecurity alerts or advisories.[4]

For the year ending March 31, 2021, the Office of the Privacy Commissioner of Canada received 782 breach reports, affecting at least 9 million Canadian accounts, mainly in the financial, telecommunications, retail, insurance, and services sectors. 64% were due to unauthorized access by threat actors, often through social engineering. 42% of the breaches were accomplished with such attack vectors as malware (malicious software), ransomware, password attacks, and credential stuffing attacks (see Definitions and Descriptions below).[5]

Cybersecurity breaches can entail significant business, financial, and reputational consequences. According to IBM, in 2022 Canada had the third highest costs for cyberbreaches, with an average estimated cost of $5.64M US per breach,[6] but 2021 saw one of the largest U.S. insurance companies, CNA Financial Corp., pay $40 million in ransom alone.[7] That does not include the business disruption and system repair costs.

In Canada, Home Hardware, Humber River Hospital (Toronto), Discount Car and Truck Rentals, and the Sault Ste. Marie Police Service in Ontario were all victims of ransomware attacks in 2021.[8]

3. A Government of Canada agency launched in 2018: https://cyber.gc.ca/en/about-cyber-centre, accessed July 9, 2022. The Canadian Centre for Cyber Security, also called the Cyber Centre, is part of the Communications Security Establishment, the Government of Canada's agency responsible for information technology security and foreign signals intelligence, under the Minister of National Defence: https://www.cse-cst.gc.ca/en/culture-and-community/history/our-story#tcc, accessed November 24, 2022.
4. https://cyber.gc.ca/en/alerts-advisories, accessed November 24, 2022.
5. Office of the Privacy Commissioner of Canada, *2020-2021 Annual Report to Parliament on the Privacy Act and the Personal Information Protection and Electronic Documents Act*, https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/ar_202021, accessed November 24, 2022.
6. IBM Corporation, *Cost of a Data Breach Report 2022*, July 2022, https://www.ibm.com/security/data-breach, accessed November 24, 2022.
7. "CNA Financial Paid $40 Million in Ransom After March Cyberattack", *Bloomberg*, 20 May 2021. https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack accessed November 24, 2022.
8. Howard Solomon, 2021: "'A crazy mess': Cybersecurity year in review and a

Early that year, and again towards year's end, Canada Revenue Agency (CRA) denied taxpayers access to its systems because of security incidents.[9]

Lawyers and law firms have not been spared. Stateside, the American Bar Association reports that 25% of law firms canvassed reported a data breach at some time in 2021.[10] Meanwhile, in Canada, as early as 2011, reports emerged of "at least seven of Canada's leading law firms" being targeted by attacks in relation to the failed $38 billion takeover bid for the Potash Corporation of Saskatchewan Inc.[11] More recently, the authors of "Cybersecurity and Law Firms" observed:[12]

> Law firms have become attractive targets for cyberattacks as lawyers have access to and store clients' confidential information. Several prominent Bay Street law firms working on a [Potash Corporation of Saskatchewan Inc.] takeover were attacked by hackers, apparently based in China, in an attempt to frustrate the deal. The attackers used phishing techniques to send emails to law firms and government officials purporting to be from trusted officials' accounts. Once the attachments were opened, they spread malware in the computer network designed to gather and leak information on the potash transaction. The Boston Business Journal highlighted the potential risks the ten largest Boston intellectual property law firms face to cyberattacks and the leakage of sensitive data. The journal pointed out that law firms are increasingly at risk of cybersecurity breaches. Notably, Cisco's 2015 Annual Security Report ranked law firms as the seventh highest sector to be a target of cyberattack in 2014.

Having established that the threats to, and need for, cybersecurity are real, we next look at just what "cybersecurity" means.

look ahead", *ITWorld Canada*, December 31, 2021, https://www.itworldcanada.com/article/2021-a-crazy-mess-cybersecurity-year-in-review-and-a-look-ahead/469389, accessed November 24, 2022.

9. See https://www.canada.ca/en/revenue-agency/news/2021/03/accounts-locked-on-february-16.html and https://www.canada.ca/en/revenue-agency/services/e-services/updates.html, accessed November 24, 2022.
10. David G. Ries, "2021 Cybersecurity", *ABA Tech Report 2021*, https://www.americanbar.org/groups/law_practice/publications/techreport/2021/cybersecurity, December 22, 2021, accessed November 24, 2022.
11. "Foreign hackers targeted Canadian firms", November 29, 2011, https://www.cbc.ca/news/politics/foreign-hackers-targeted-canadian-firms-1.1026810, accessed November 24, 2022.
12. Bryan P Schwartz *et al.*, "Cybersecurity and Law Firms", *Asper Review of International Business and Trade Law*, Volume 21 Special Edition – 2021, CanLIIDocs 988, https://canlii.ca/t/t58s, accessed November 24, 2022.

A. Cybersecurity: A Definition

We adopt here the definition of "cybersecurity" and related terms from CyberSecure Canada,[13] the Government of Canada's (via Innovation, Science and Economic Development Canada)[14] cybersecurity certification program:[15]

> Cybersecurity is the protection of data, information, computers, devices and networks from cyber threats and attacks. [...] A cyber threat is an activity intended to compromise the security of your cyber threat environment by changing the availability, integrity or confidentiality of your systems or the information they contain. [...] A cyber threat environment is the online space where malicious cyber threat activity can occur.

B. Attack Vectors

Although cybersecurity attack vectors, or cyber threats, are relatively recent phenomena,[16] the list of their names and types is long and still growing.

The following is a highly selective, and plainly non-exhaustive, list of definitions and descriptions of some of the current key cyber threats:[17]

Business Email Compromise (BEC)

Emails designed to trick employees in a target organization into transferring funds to cyber threat actors (often) impersonating high-level executives or trusted third parties.

Code Injection

The introduction of malicious code into a computer program by exploiting flaws in a program's functionality instructions or data

13. Canada, "CybserSecure Canada" (February 2022), https://www.ic.gc.ca/eic/site/137.nsf/eng/home, accessed November 24, 2022.
14. Canada, "Innovation, Science and Economic Development Canada" (April 2022), online: https://www.ic.gc.ca/eic/site/icgc.nsf/eng/home, accessed November 24, 2022.
15. https://ised-isde.canada.ca/site/cybersecure-canada/en/why-certification-matters/what-cybersecurity, accessed November 24, 2022.
16. Pogrebna, Ganna and Mark Skilton, "Cybersecurity Threats: Past and Present", Navigating New Cyber Risks (2019).
17. Our list is based on the Cyber Centre's *Cyber Threat Toolbox*. See: Canada, Canadian Centre for Cyber Security, "An introduction to the cyber threat environment" (June 2021), online: https://cyber.gc.ca/en/guidance/annex-cyber-threat-toolbox#shr-pg0, accessed November 24, 2022.

input interpretation. Two common code injection techniques are cross-site scripting (XSS) and Structured Query Language (SQL) injection.

. XSS: a threat actor injects and executes malicious code within a web application by bypassing input validation mechanisms. The browser executes the malicious code, accessing the exploited web application. XSS-injected code may be a one-time execution or stored for future use.

. SQL injection: a threat actor retrieves or modifies the contents of an SQL database by entering code into web forms meant to receive input for or query SQL databases. These databases may hold personally identifiable or other sensitive information.

Credential Stuffing

Cyber threat actors use lists of stolen username and password combinations to gain unauthorized access to online accounts. They run large-scale automated login requests, hoping that one of the compromised username/password pairs will match an existing account on the site and give them access. 1.8 billion credential pairs were stolen in 2021, and credential stuffing remains widespread.[18]

Distributed Denial of Service (DDoS)

A widely used threat vector. Threat actors disrupt the activities of a host (*e.g.*, website, server, network, Internet of Things device) by overwhelming it, often from a botnet (a network ofmalware-infected computers), with a flood of Internet traffic, also known as requests. The objective is to render the host unavailable for legitimate requests from users, leaving the targeted system dysfunctional. DDoS attacks are hard to stop, and difficult to distinguish from legitimate user traffic.

Drive-by Exploit (Watering Hole)

Malicious code that a cyber threat actor places on a website without the website host's knowledge. The malicious code

18. Sander Vinberg and Jarrod Overson, "2021 Credential Stuffing Report", (9 February 2021), *F5 Labs,* online: https://www.f5.com/labs/articles/threat-intelligence/2021-credential-stuffing-report, accessed November 24, 2022.

compromises the devices of any user who visits the website. A Watering Hole is a drive-by attack targeting a specific website frequented by individuals.

Password Cracking

A method to access accounts directly. Two common forms of password cracking are "brute force" and "dictionary-based". Brute force cracking takes advantage of computer processing speed and power and pumps out endless randomly generated passwords to try to gain access. Dictionary-based cracking checks against a list of commonly used passwords ("123456" remained the most common password in 2021, used over 100 million times across the planet).[19]

Person-in-the-middle (PITM)

A threat actor intercepts a communication between parties, for example, as a victim and a web server, without the victim's knowledge. The victim believes that they are communicating directly and securely with the website. However, PITM allows the threat actor to monitor communications, reroute traffic, alter information, deliver malware, and acquire sensitive information. PITM is achieved via several techniques, such as phishing, Wi-Fi eavesdropping, and SSL hijacking.

Phishing

A widespread social engineering technique by which threat actors disguise themselves as a trustworthy entity, tricking recipients into giving up information, such as login credentials, banking details, and other valuable or sensitive data. Usually conducted through email spoofing and phony text messages. Users become victims when they open malicious attachments or click on misleading, embedded links.

Ransomware

A pervasive and disruptive attack vector. It is "the foremost cyber threat facing Canadians and Canadian organizations".[20] Ransomware is malware that makes computer data inaccessible

19. "Top 200 most common passwords"(2002), *NordPass*, online: https://nordpass.com/most-common-passwords-list/, accessed November 24, 2022.
20. Canadian Centre for Cyber Security, "Cyber threat bulletin: The ransom-ware threat in 2021" (December 2021), online: https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-ransomware-threat-2021 #fn6-rf, accessed November 24, 2022.

until the victim pays a ransom. The ransomware either encrypts the data or locks the user out of their system until the ransom is paid, usually via a cryptocurrency such as bitcoin. Once the ransom is paid, the threat actor (usually) delivers the key to unlocking the data or system. Threat actors may also threaten to expose sensitive information unless a ransom is paid. Ransomware is typically installed via phishing or compromised websites.

Social Engineering

Manipulation of a user to gain access to personal information and protected systems. Common examples are phone calls, phishing emails, or bogus ("smishing") texts in which threat actors pretend to be the Canada Revenue Agency or a bank, for example, and trick the user into giving up their account access information.

Spear Phishing

Another social engineering technique. A cyber threat actor sends a personally tailored phishing message to a precisely selected recipient or set of recipients. They use details believable to the target as originating from a trusted source.

Spoofing

The act of masking or forging a website, email address, or phone number to appear as if it originates from a trusted source. After receiving a phishing message, the victim can be enticed into giving away personal, financial, or other sensitive information or clicking on a link or attachment, which can infect a device with malware.

Spyware

Malware used to track computer users, often without the user's knowledge or consent (a major exception being its use by employers to track employees).[21] Spyware can monitor keystrokes, capture data, access a computer's microphone and webcam, generally track user activity and surfing habits, and capture usernames and passwords.

21. *Employment Standards Act, 2000*, SO 2000, c 41, Part XI.1.

Typo-squatting (or URL Hijacking)

A threat actor registers domain names with misspellings resembling a legitimate domain address to confuse users. "Googgle" instead of "Google", or "Amzaon" instead of "Amazon" for example. This allows the threat actor to redirect users who mistype a web address to a malicious look-alike domain under the threat actor's control. The new domain can deliver malware and acquire personally identifiable or other sensitive information.[22]

Virus, Worm, Trojan

Malware is commonly delivered through viruses, worms, and trojans. A virus is a program that inserts its own code into legitimate programs to damage the host computer, for example, by deleting files and programs, or corrupting storage and operating systems. A worm is a program meant to self-replicate and spread to other computers, drain system resources, and propagate code (the payload) to damage its host. A trojan is malware disguised as, or embedded in, legitimate software, with similar objectives as viruses and worms, but without replicating or propagating on its own.

WI-FI Eavesdropping

A threat actor installs a seemingly legitimate Wi-Fi network in a public area, for example naming it "Free Wi-Fi". By connecting, the user is now victim to a person-in-the-middle (PITM) attack. The threat actor can monitor their communications and acquire personal and other sensitive information.

Zero-day Vulnerabilities

Software vulnerabilities or bugs known only to a few people, which allows them to exploit the vulnerabilities before they can be patched by the software publisher.

22. For an especially malicious example of this attack vector using foreign alphabets, see Brian Krebs, "Disneyland Malware Team: It's a Puny World After All", November 16, 2022, https://krebsonsecurity.com/2022/11/disneyland-malware-team-its-a-puny-world-after-all, accessed November 24, 2022.

This chart from the ISACA Journal[23] is a convenient summary, and expansion, of the attack vectors just described:[24]

Figure 1—Cybersecurity Attack Vectors

Cyberattack Vector	Examples/Description	Objective	Problem Identifier
Malware	Virus, worm, trojan horse, spyware, rootkit software	Data theft, password stealer, network or system compromise	Antivirus software; intrusion detection system (IDS)
Phishing (includes spear phishing)	Deceptive malicious email that targets organizational users and uses attachments or malicious links to plant malware	Network or system access; data breach	User
Ransomware (includes doxing)[a]	Extortion (data are deleted or encrypted unless ransom is paid)	Blackmail for ransom	Ransomware announcement
Denial of service (DoS) (includes distributed DoS [DDoS])	Overwhelm network device or server to prevent access or usage	Network or system disruption	Network administrators via network monitoring system
Compromised, weak or stolen credentials	User login account and password	Data breach	Forensic investigation
Malicious insiders	Disgruntled employee who exposes private information	Revenge, embarrassment	Management, United States Computer Emergency Readiness Team (US-CERT)
Third- and fourth-party vendors	Suppliers, cybersecurity partners	Obtain competitive information	Network monitoring system; log management system
Missing or poor encryption	Data at rest, data in motion	Gain access to data	System assessment
Device misconfiguration	Servers, network devices, mobile computing devices	Obtain access to device and data	System assessment
Unpatched vulnerabilities	Servers, network devices, mobile computing devices	Obtain access to device and data	Patch management system
Structured Query Language (SQL) injections	Manipulate database servers to expose information	Gain access to data	Penetration tester
Cross-site scripting	Inject malicious code into a comment	Gain access to system, network and data	Penetration tester
Session hijacking	Intercepted session cookies	Gain access to data	User
Man-in-the-middle (MitM) attacks	Public Wi-Fi networks	Gain access to network	Intrusion prevention system (IPS)
Brute-force attack	Trial-and-error attempts to gain access to network or system	Gain access to system, network and data	Log management system

23. ISACA (isaca.org) is the technology professionals' organization formerly known as the Information Systems Audit and Control Association.
24. Larry G. Wlosinski, "Cybersecurity Incident Response Exercise Guidance", online: (2022) ISACA Journal, 1, https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance, accessed November 24, 2022.

Legislating Cybersecurity: The Statutory Framework

A. Overview: Data Protection and Privacy Laws

Canadian legislatures have created a complex of data protection laws that address privacy concerns over the collection, use or disclosure of personal information. This gives rise to varied potential remedies for data breaches from administrative, regulatory, or civil parties, depending on the type of personal information and on the sphere in which the personal information originates.

Canadian legislation distinguishes the personal information privacy obligations between private organizations and public bodies. The *Personal Information Protection and Electronic Documents Act* (*PIPEDA*)[25] governs the commercial activity of the former (along with several sector-specific and provincial counterparts), while public bodies are governed by the federal *Privacy Act*,[26] along with some statutes specific to provincial public actors.

The federal and provincial statutory regimes in both the private and public spheres, protect the collection, use and disclosure of "personal information".[27] It is thus important to understand what "personal information" is.

The Federal Court of Canada has applied a broad and purposive approach to privacy statutes, and interpreted "personal information" as deliberately broad.[28] Generally speaking, courts have considered information to be "personal information" if it is about an "identifiable individual", meaning that the individual can be identified by combining the disclosed information with publicly available information.[29] Anyone wishing to demonstrate that

25. SC 2000, c 5.
26. RSC 1985, c. P-21.
27. Charnetski, *The Personal Information and Electronic Documents Act, A Comprehensive Guide* (Aurora: Canada Law Book, 2001) at 203.
28. *Canada (Privacy Commissioner) v. Canada (Labour Relations Board)*, [19961 3 F.C. 609, 41 Admin. L.R. (2d) 49, 118 F.T.R. 1 (Fed. T.D.) at para. 48, affirmed (2000), 25 Admin. L.R. (3d) 305, 25 Admin. L.R. 305, 2000 C.L.L.C. 220-037 (Fed. C.A.).
29. *Girao v. Zerek Taylor Grossman Hanrahan LLP*, 2011 FC 1070, 338 D.L.R. (4th) 262, 96 C.P.R. (4th) 220 (F.C.) at para. 32, referencing *Canada (Information Commissioner) v. Canadian Transportation Accident Investigation & Safety Board*, 2005 FC 384, 40 C.P.R. (4th) 158, [20061 1 F.C.R. 605 (F.C.) at para. 43, reversed 2006 FCA 157, 267 D.L.R. (4th) 451, 49 C.P.R. (4th) 7 (F.C.A.), leave to appeal refused (2007), 368 N.R. 396 (note), 2007 CarswellNat 800, 2007 CarswellNat 801 (S.C.C.).

information about an identifiable individual is not personal information must show that some form of exception applies.[30]

The litigation consequences of cyberbreaches are at least partly rooted in the complex statutory framework for data protection and cybersecurity. The right parties must take the right steps at the right times. Liability may result otherwise.

B. Federal Legislation

Federally, data protection and cybersecurity are governed by a small, but far-reaching number of statutes, with some yet-to-be filled legislative gaps. As at this writing, new legislative developments are on the table (discussed below). Cybersecurity and cyberbreach laws– and by extension the relevant litigation avenues – are set to undergo much evolution in the near future.

What follows is a snapshot of the legislative *status quo*.

i. Private Sector

PIPEDA

Statutory Framework

PIPEDA is Canada's privacy legislation for private commercial entities. Federal courts have described it as a "compromise both as to substance and to form", balancing individual privacy interests with the commercial needs of organizations.[31]

PIPEDA states its purpose to be a response to an "era in which technology increasingly facilitates the circulation and exchange of information".[32] However, its genesis is coextensive with international forces, beginning with privacy legislation in the European Union.[33] Now over 20-years old, *PIPEDA* is in need of much fine-tuning and updating (more on this below).

---

30. *Sutherland v. Canada (Minister of Indian & Northern Affairs)* (1994), 115 D.L.R. (4th) 265, [19941 3 F.C. 527, [19951 1 C.N.L.R. 195 (Fed. T.D.), at para. 22.

31. *Englander v. Telus Communications Inc.*, 2004 FCA 387, 247 D.L.R. (4th) 275, 36 C.P.R. (4th) 385 (F.C.A.), at para. 38; *Johnson v. Bell Canada*, 2008 FC 1086, 299 D.L.R. (4th) 296, 70 C.P.R. (4th) 1 (F.C.), at para. 21.

32. *PIPEDA*, s 3.

33. In 1995, the European Commission established *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, s 57*, Article 25.1-25.2. This was superseded by

PIPEDA governs the collection, use and disclosure of personal information by organizations "in the course of commercial activities".[34] It also governs personal information that is about an employee of, or an applicant for employment with, the organization, and information that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business.[35] The statute applies not only to federal works and undertakings, but also undertakings that occur wholly within provinces without legislation deemed to be "substantially similar" to *PIPEDA*.[36]

PIPEDA states that it applies to "organizations". The statute broadly defines the term as including associations, partnerships, persons (such as corporations) and trade unions.[37] "Commercial activity" is more difficult to identify. Under the statute, it is defined as any particular transaction, act, or regular course of conduct that is of a commercial character.[38] However, the Office of the Privacy

---

European Union, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2017 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, Article 44.

34. *PIPEDA*, s 4(1)(a), (b). For the influence of the Canadian Standards Association on the genesis of *PIPEDA*, see *Statutory Review Of The Personal Information Protection And Electronic Documents Act (Pipeda)*, Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics, May 2007, footnote 4, https://www.ourcommons.ca/Content/Committee/391/ETHI/Reports/RP2891060/ethirp04/ethirp04-e.pdf, accessed November 27, 2022.
35. *Ibid.*
36. *PIPEDA*, s 26(2).
37. *PIPEDA*, s 2(1). It remains to be seen how broadly this definition will be stretched beyond traditional examples of commercial organizations. For example, the Office of the Privacy Commissioner recently concluded that *PIPEDA* does not apply to the Canadian federal political parties. See: Office of the Privacy Commissioner of Canada, *Letter Regarding Complaint Against Federal Political Parties* (March 25, 2021), online: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/let_pol_210325. The political parties' exemption may not last, however. Recent decisions from the Information and Privacy Commissioner of British Columbia have found the federal political parties to be "organizations" within the meaning of the province's *Personal Information Protection Act*, SBC c 63 (BC *PIPA*): *Courtenay-Alberni Riding Assn. of The New Democratic Party of Canada*, 2019 BCIPC 34, 2019 CarswellBC 2581, [20191 B.C.I.P.C.D. No. 34 (B.C. Information & Privacy Commr.); *Conservative Party of Canada, Re*, 2022 BCIPC 13, 2022 CarswellBC 593, [20221 B.C.I.P.C.D. No. 13 (B.C. Information & Privacy Commr.).
38. *PIPEDA*, s 2(1).

Commissioner of Canada has noted that, even without a direct commercial link, an activity may still be commercial depending on the nature of the organization's business.[39]

Organizations across Canada are covered by *PIPEDA*, except in provinces that have enacted substantially similar privacy legislation. At present, only three provinces have done so: Québec, Alberta, and British Columbia.[40]

PIPEDA defines "personal information" as "information about an identifiable individual".[41] The definition is "very elastic".[42] The Federal Court has ruled that it is unclear what *PIPEDA*'s definition of "personal information" captures, although it must be "about" an identifiable individual.[43] For example, while an individual's first name may not constitute personal information on its own, if the name can be used with other information to lead back to an individual, it will be considered personal information.[44] The Office of the Privacy Commissioner has provided similar guidance on the nature of personal information.[45]

39. See for example: Office of the Privacy Commissioner of Canada, *PIPEDA Report of Findings #2009-008: Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act* at paras 11-12, online: https://www.priv.gc.ca/en/opc-ac-tions-and-decisions/investigations/investigations-into-businesses/2009/ pipeda-2009-008, accessed November 24, 2022.
40. *PIPEDA*, s 26(2); *Organizations in the Province of Québec Exemption Order*, SOR/2003-374; *Organizations in the Province of Alberta Exemption Order*, SOR/2004-219; *Organizations in the Province of British Columbia Exemption Order*, SOR/2004-220. New Brunswick, Newfoundland, Nova Scotia and Ontario also have provincial health information laws substantially similar to PIPEDA that apply to personal health information within those provinces.
41. *PIPEDA*, s 2(1).
42. *Citi Cards Canada Inc. v. Pleasance*, 2011 ONCA 3, 328 D.L.R. (4th) 707, 4 C.P.C. (7th) 264 (Ont. C.A.) at para. 22, overturned on other grounds: *Royal Bank of Canada v. Trang*, 2016 SCC 50, [2016] 2 S.C.R. 412, 403 D.L.R. (4th) 193 (S.C.C.), at paras. 28-29.
43. *Girao, supra*, at para 32.
44. Office of the Privacy Commissioner, *PIPEDA Case Summary #2002-54: Couple alleges improper disclosure of telephone records to a third party*
45. In its guide for organizations complying with *PIPEDA*, the OPC defined "personal information" as any factual or subjective information, recorded or not, about an identifiable individual, which could be in such forms as age, ID numbers, income, ethnic origin, blood type, opinions, evaluations, comments, social status, disciplinary actions, employee files, credit records, loan records, medical records, existence of a dispute between a consumer and merchant or intentions (such as to acquire goods or services). OPC, "Summary of privacy laws in Canada" (1 January 2018), online:

PIPEDA does not apply, however, to specific types of information, such as:[46]

(a) information collected, used, or disclosed by an individual for personal or domestic purposes or by an organization for journalistic, artistic, or literary purposes;[47]
(b) an individual's "business contact information" that an organization collects, uses or discloses in order to communicate with the individual in relation to their employment, business, or profession;[48] and
(c) the core activities of municipalities, universities, schools, and hospitals, unless they are engaged in commercial activity.[49]

An organization's collection, use or disclosure of personal information must be for purposes that a reasonable person would consider appropriate in the circumstances.[50] The legal test for reasonableness is composed of four questions:

(a) is the collection, use or disclosure of personal information necessary to meet a specific need?
(b) is the collection, use or disclosure of personal information likely to be effective in meeting that need?
(c) is the loss of privacy proportional to the benefit gained?
(d) is there a less privacy-invasive way of achieving the same end?[51]

https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15, accessed November 24, 2022.

46. In addition to the listed exceptions, PIPEDA, s 7 and Regulation SOR/2001-7 under PIPEDA set out several exceptions to its consent requirement.
47. *PIPEDA*, s 4(2).
48. *PIPEDA*, s 4.01.
49. Office of the Privacy Commissioner of Canada, *The Application of PIPEDA to Municipalities, Universities, Schools and Hospitals*, December 2015, online: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/02_05_d_25/, accessed November 24, 2022.
50. *PIPEDA*, s 5(3). This has been described by the Supreme Court of Canada as "a guiding principle that underpins the interpretation of the various provisions of *PIPEDA*", *R. v. Spencer*, 2014 SCC 43, [20141 2 S.C.R. 212, 375 D.L.R. (4th) 255 (S.C.C.), at para. 63. See also Office of the Privacy Commissioner of Canada, Guidance on inappropriate data practices: Interpretation and application of subsection 5(3), https://www.priv.gc.ca/ en/privacy-topics/collecting-personal-information/consent/gd_53_201805/ #fn7-rf, accessed November 27, 2022.
51. *Mountain Province Diamonds Inc. v. De Beers Canada Inc.*, 2014 ONSC 2026, 25 B.L.R. (5th) 141, 239 A.C.W.S. (3d) 226 (Ont. S.C.J.), at para. 47, citing *Eastmond v. Canadian Pacific Railway*, 2004 FC 852, 33 C.P.R. (4th) 1, [20051 2 F.C.R. D-32 (F.C.), at para. 13.

Organizations are responsible for the personal information under their control. They must designate an individual or individuals who are accountable for the principles set out in Schedule 1 of *PIPEDA* and must abide by the obligations set out in that Schedule.[52] Simplifying, the principles under Schedule 1 mandate:

(a) **accountability** organizations must be accountable for collecting, using or disclosing personal information under their control;[53]

(b) **identifying purposes** individuals must be provided with an identified purpose for the collection, use or disclosure of their information at or before the time of collection;[54]

(c) **consent** organizations must obtain consent from individuals, consider their reasonable expectations, and provide an opportunity to withdraw consent at any time;[55]

(d) **limiting collection** organizations must limit collection, retention or disclosure to personal information that is required for purposes properly identified by an organiza-tion;[56]

(e) **limiting use, disclosure, and retention** organizations must limit their use, disclosure and retention of personal information to purposes for which it was collected, except with consent, as required by law or in accordance with subsections 7(2) and (3) of *PIPEDA*;[57]

(f) **accuracy** personal information must be accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used;[58]

(g) **safeguards** personal information must be protected by security safeguards appropriate to the sensitivity of the information;[59]

(h) **openness** organizations shall make specific information about their policies and practices relating to the management of personal information readily available to individuals;[60]

52. Schedule 1 of *PIPEDA* incorporates the *National Standard of Canada Entitled Model Code for the Protection of Personal Information*, CAN/CSA-Q830-96, a set of 10 principles for the collection, use and disclosure of personal information which significantly pre-date *PIPEDA*. Under s 5(1), *PIPEDA* mandates that all organizations must comply with this code.

53. *PIPEDA*, Schedule 1, Article 4.1.

54. *Ibid.*, Article 4.2.

55. *Ibid.*, Article 4.3.

56. *Ibid.*, Article 4.4.

57. *Ibid.*, Article 4.5.

58. *Ibid.*, Article 4.6.

59. *Ibid.*, Article 4.7.

(i) **individual access** upon request, an individual must be informed of the existence, use and disclosure of personal information, shall be given access to that information and shall be able to challenge the accuracy and completeness of that information and have it amended if appropriate;[61] and

(j) **challenging compliance** an individual shall be able to address a challenge concerning compliance with the above principles to the designated individual (or individuals) accountable for an organization's compliance.[62]

The seventh principle under Schedule 1 *safeguards* is especially relevant to cybersecurity. Under the principle, organizations must protect personal information, regardless of the format in which it is held, with security safeguards tailored to the information's sensitivity, to protect against loss or theft, as well as unauthorized access, disclosure, copying, use or modification.[63]

These protections should include physical measures, such as locked cabinets; organizational measures, such as security clearances; and technological measures, such as the use of passwords or encryption.[64]

Following amendments in June 2015, *PIPEDA* now requires organizations to notify the Commissioner, affected individuals, and organizations or government institutions that may be able to reduce or mitigate the risk of harm, if it is reasonable to believe that a breach of security safeguards poses a "real risk of significant harm" to the affected individuals.[65]

"Significant harm" is defined broadly as including bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on credit records, and damage to or loss of property.[66]

Factors to consider when assessing the real risk of significant harm will include: (a) the sensitivity of the personal information involved in the breach; (b) the probability that the personal information has been, is being, or will be misused; and (c) any other prescribed factor under the legislation.[67]

60. *Ibid.*, Article 4.8.
61. *Ibid.*, Article 4.9.
62. *Ibid.*, Article 4.10.
63. *Ibid.*, Article 4.7.
64. *Ibid.*, Article 4.7.3.
65. *PIPEDA*, s 10.1.
66. *Ibid.*, s 10.1(7).
67. *Ibid.*, s 10.1(8).

Similarly, an organization must keep records of every breach of security safeguards involving personal information under its control.[68] Failure to do so can attract prosecution as a summary conviction or indictable offence, and a fine of up to $100,000.[69] To make expectations clearer, the Commissioner has published a directive on these reporting requirements.[70]

As awareness and understanding of cybersecurity risks and organizations' use of personal data grows, it will be interesting to see how expectations around the reasonableness standard for personal information safeguards evolve.

Breach of PIPEDA: Remedies

PIPEDA offers different remedies for violations of its provisions.

Complaint: First, an individual may file a complaint with the federal Privacy Commissioner for breach of Division 1 (protection of personal information), Division 1.1 (breaches of security safeguards), or Schedule 1 of *PIPEDA*.[71] The Commissioner has the authority to receive complaints, conduct investigations – including Commissioner-initiated ones – and issue reports on their findings.[72] Upon receiving a complaint, the Commissioner must investigate it, except where (i) the complainant has not exhausted reasonable and available grievance procedures,[73] (ii) procedures under federal or provincial laws are more appropriate for dealing with the complaint,[74] or (iii) the complaint was not filed within a reasonable time.[75] The Commissioner's investigative powers are

---

68. *Ibid*, s. 10.3(1). Section 10.3(2) allows the Commissioner to compel an organization to provide the record of any breach, not just those that pose a real risk of significant harm.
69. *Ibid*, s. 28(b).
70. Office of the Privacy Commissioner of Canada, "What you need to know about mandatory reporting of breaches of security safeguards" (October 2018, revised August 13, 2021), online: https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/, accessed November 24, 2022.
71. *PIPEDA*, s 10.
72. *PIPEDA*, ss 11(1)-(2).
73. *Eastmond*, *supra*.
74. Office of the Privacy Commissioner, *PIPEDA Case Summary #2010-001, Commissioner does not issue report to individual seeing access to her personal information being withheld for reasons of solicitor-client privilege,* online: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2010/pipeda-2010-001/, accessed November 24, 2022.
75. *PIPEDA*, s 12(1).

extremely broad, extending to foreign entities with no facilities in Canada.[76]

A complainant may challenge a matter subject to a complaint or referred to in the Commissioner's report by application to the Federal Court,[77] or seek judicial review of the Commissioner's report after exhausting the avenues under section 14 of *PIPEDA*.[78] The standard of review in such circumstances is presumptive reasonableness, since the Supreme Court of Canada's decision in *Canada (Minister of Citizenship and Immigration) v. Vavilov*.[79]

Alternatively, the Commission may apply to the Federal Court for a hearing either with the consent of the complainant, on behalf of the complainant, or with leave of the Federal Court.[80]

Several investigations into large-scale data breaches contravening *PIPEDA* have been particularly high-profile, including investigations into:

(a) Clearview AI, Inc., to determine whether its collection, use and disclosure of personal information by means of facial recognition tools complied with federal and provincial private sector privacy laws (conducted jointly with the Alberta, BC, and Québec privacy commissioners);[81]

(b) Fédération des caisses Desjardins du Québec, for breach of security safeguards that affected close to 9.7 million individuals in Canada and abroad, with compromised

76. *Lawson v. Accusearch Inc.*, 2007 FC 125, 280 D.L.R. (4th) 358, [20071 4 F.C.R. 314 (F.C.).

77. *PIPEDA*, s 14, with contravention required of ss "4.1.3, 4.2, 4.3.3, 4.4, or 4.6 to 4.8 of Schedule 1, in s 4.3, 4.5 or 4.9 of that Schedule as modified or clarified by Division 1 or 1.1, as well as ss 5(3), 8(6)-(7), 10 in Division 1.1.

78. *Kniss v. Canada (Privacy Commissioner)*, 2013 FC 31, 425 F.T.R. 137 (Eng.), 224 A.C.W.S. (3d) 802 (F.C.).

79. 2019 SCC 65, [20191 4 S.C.R. 654, 441 D.L.R. (4th) 1 (S.C.C.), at para. 10. This presumption is rebutted where there is a clear indication of legislative intent or otherwise, or the rule of law requires the standard of correctness to be applied because of a constitutional question, a general question of law of central importance to the legal system, or a question related to the jurisdictional boundaries between administrative bodies. In the *PIPEDA* context, see for example: *Witty v. Mississauga First Nation*, 2021 FC 436, 331 A.C.W.S. (3d) 778, 2021 CarswellNat 2076 (F.C.).

80. *PIPEDA*, s 15.

81. *PIPEDA* Findings 2021-001, *Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accês a` l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta* (2021 Feb 2), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/, accessed November 24, 2022.

personal information such as names, dates of birth, social insurance numbers, contact information, and transaction histories;[82]

(c) Equifax Inc. and Equifax Canada Co.'s compliance with *PIPEDA*, regarding breach of security safeguards resulting in the disclosure of personal information in 2017 relating to nearly 19,000 individuals;[83] and

(d) The adult website Ashley Madison, in connection with hacking and online posting of user's account information (jointly with the Australian Privacy Commissioner).[84]

Damages: Second, individuals may pursue damages. The Federal Court may (i) order an organization to correct its practices under *PIPEDA*, (ii) order an organization to publish a notice of action taken or proposed to be taken, or (iii) award damages or "any other remedies".[85] Historically, the Federal Court has only awarded damages where the breach of *PIPEDA* is of a serious and violating nature.[86]

The Federal Court's damages awards under *PIPEDA* are typically modest, including:

(a) $1,500 for unauthorized publication of the Privacy Commissioner's report that a complaint was not well-founded;[87]

(b) $5,000 for disclosing incorrect information about an appli-cant's credit score;[88]

82. *PIPEDA* Findings 2020-005, *Investigation into Desjardins' compliance with PIPEDA following a breach of personal information between 2017 and 2019* (2020 December 14), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-005/, accessed November 24, 2022.

83. *PIPEDA* 2019-001, *Investigation into Equifax Inc. and Equifax Canada Co.'s compliance with PIPEDA in light of the 2017 breach of personal information* (2019 April 9), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-001/, accessed November 24, 2022.

84. *PIPEDA* 2016-005, *Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/Acting Australian Information Commissioner* (2016 August 22), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2016/pipeda-2016-005/, accessed November 24, 2022.

85. *PIPEDA*, s 16.

86. *Randall v. Nubodys Fitness Centres*, 2010 FC 681, 371 F.T.R. 180, 190 A.C.W.S. (3d) 938 (F.C.), at paras. 54-55; *Townsend v. Sun Life Financial*, 2012 FC 550, 103 C.P.R. (4th) 424, 408 F.T.R. 279 (Eng.) (F.C.).

87. *Girao*, *supra*.

88. *Nammo v. Transunion of Canada Inc.*, 2010 FC 1284, [2012] 3 F.C.R. 600, 379 F.T.R. 130 (Eng.) (F.C.), at para. 79.

(c) $5,000 for making a complainant's litigation-related information easily searchable on a paid-services website;[89] and
(d) over $20,000 for a telecommunications provider's failure to highlight its policy of authorizing a credit check that could impact an applicant's credit score.[90]

These awards have been largely individual-focused, distinct from the mass-data breaches that have made headlines in recent years. Whether the awards will be higher for mass-data breaches remains unknown. Given the scale of such breaches, it would not be surprising if they were, if only to add a deterrence factor to *PIPEDA* damages awards, alongside the compensatory one.

Whether the jurisdiction over breaches of *PIPEDA* extend to provincial courts is unclear. Judges have disagreed.

On one hand, the British Columbia Supreme Court, followed by the Ontario Superior Court of Justice, has ruled that *PIPEDA* does not create a statutory cause of action enforceable by provincial superior courts; rather, jurisdiction rests exclusively with the Privacy Commissioner and the Federal Court.[91]

Similarly, in *Kaplan v. Casino Rama*, Justice Belobaba refused to certify a class action over the hacking of Casino Rama's computer system and the theft of personal information. His Honour noted the option of pursuing damages under *PIPEDA*, but only with reference to the Federal Court's powers, not the Ontario Superior Court's.[92]

On the other hand, Justice Lauwers, then in the Ontario Superior Court, granted an application for an order under section 7(3)(c) of *PIPEDA*, requiring a credit union to disclose personal information.[93] Similarly, the Supreme Court has found the

---

89. *T. (A.) v. Globe24h.com*, 2017 FC 114, 407 D.L.R. (4th) 733, 143 C.P.R. (4th) 483 (F.C.), at para. 103.

90. *Chitrakar v. Bell TV*, 2013 FC 1103, 441 F.T.R. 254 (Eng.), 234 A.C.W.S. (3d) 1057 (F.C.), at para. 28.

91. *Yakobi v. Canadian Imperial Bank of Commerce*, 2007 BCSC 923, 159 A.C.W.S. (3d) 416, 2007 CarswellBC 1495 (B.C. S.C.); also see: *Lee v. Magna International Inc.*, 2019 ONSC 102, 53 C.C.E.L. (4th) 147, 301 A.C.W.S. (3d) 303 (Ont. S.C.J.) at para. 60, additional reasons 2019 ONSC 1300, 53 C.C.E.L. (4th) 163, 302 A.C.W.S. (3d) 473 (Ont. S.C.J.); *Wilson v. Bourbeau* (2009), 249 O.A.C. 122, 177 A.C.W.S. (3d) 272, 2009 CarswellOnt 2583 (Ont. Div. Ct.), at para. 56.

92. *Kaplan v. Casino Rama*, 2019 ONSC 2025, (*sub nom.* Kaplan v. Casino Rama Services Inc.) 145 O.R. (3d) 736, 305 A.C.W.S. (3d) 249 (Ont. S.C.J.) at para. 88, additional reasons 2019 ONSC 3310, 306 A.C.W.S. (3d) 711, 2019 CarswellOnt 9260 (Ont. S.C.J.).

93. *Southlake Regional Health Centre Employees' Credit Union Ltd., Re*, 2012 ONSC 2530, 216 A.C.W.S. (3d) 775, 2012 CarswellOnt 5175 (Ont. S.C.J.), at paras. 1, 13; also see: *Mountain Province Diamonds Inc. v. De Beers Canada*

Ontario Superior Court to have jurisdiction to order a bank to produce a mortgage discharge statement as "an order made by the court" under s 7(3)(c).[94] Neither decision, however, involved an award of damages under PIPEDA.

New Private Sector Legislation (Past and Future)

In November 2020, after various calls to action, Canada's federal government tabled amendments to its privacy legislation in An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to another Act (Bill C-11). The proposed amendments were significant and drew mixed reactions.

Notably, Bill C-11 would have seen the enactment of the Personal Information and Data Protection Tribunal Act, establishing an eponymous tribunal.[95] This privacy-focused tribunal would hear appeals from the Privacy Commissioner's orders, and make decisions on whether to issue administrative monetary penalties against organizations.

Bill C-11 would also have enacted the Consumer Privacy Protection Act (CPPA), which would entail significant shifts in the enforcement of privacy legislation breaches. Like PIPEDA, it would have applied to organizations possessing personal information, with an identical definition of "organization" as PIPEDA's.[96] However, the penalties and tribunal powers under the CPPA were its most notable provisions.

The maximum penalty for contraventions, on a recommendation by the Privacy Commissioner to the tribunal, would be the higher of $10 million and 3% of an organization's gross global revenue in its financial year before the one in which the penalty was imposed.[97] Similarly, for other contraventions of the Act, organizations could be found guilty of either (a) an indictable offence and liable to a fine not exceeding the higher of $25 million and 5% of the organization's gross global revenue in its preceding financial year, or (b) an offence punishable on summary conviction and liable to a fine not exceeding

---

Inc., 2014 ONSC 2026, 25 B.L.R. (5th) 141, 239 A.C.W.S. (3d) 226 (Ont. S.C.J.).

94. Royal Bank of Canada v. Trang, 2016 SCC 50, [2016] 2 S.C.R. 412, 403 D.L.R. (4th) 193 (S.C.C.), at paras. 26-27, 50.

95. House of Commons of Canada, Second Session, Forty-third Parliament, 69 Elizabeth II, 2020, Bill C-11.

96. Ibid, Consumer Privacy Protection Act, s 6.

97. Ibid, s 94(4).

the higher of $20 million and 4% of the organization's gross global revenue.[98] This would be significantly more than the current maximum fine under *PIPEDA* of $100,000.

Although Bill C-11 was aimed at modernizing Canada's private sector privacy laws, the Privacy Commissioner referred to it as "a step back overall", giving consumers less control and organizations more flexibility in monetizing personal data, without increased accountability, and providing an unjustifiably narrow and protracted penalty scheme.[99]

Bill C-11 died on August 17, 2021, on the order paper– i.e., it was not passed before the dissolution of Parliament.

However, in 2022, two significant developments put new federal privacy legislation back into play. On June 14, 2022, less than a year after Bill C-11's death, Parliament introduced new federal privacy legislation: Bill C-26.[100] This new bill will enact the *Critical Cyber Systems Protection Act* (*CCSPA*). The *CCSPA* notably requires specific organizations, operating within "vital services" or "vital systems",[101] to establish a cybersecurity program regarding their "critical cyber systems". The *CCSPA* requires such cybersecurity programs to include consideration for identifying cybersecurity risks, protecting critical cyber systems, detecting cybersecurity incidents, and minimizing the impact of these incidents.[102]

The *CCSPA* will also include provisions around the mitigation of supply-chain and third-party risks,[103] reporting of cybersecurity incidents[104] and compliance with specific cyber security directions.[105] Interestingly, a "cybersecurity incident" is defined as

---

89. *Ibid*, s 125.
90. Office of the Privacy Commissioner of Canada, *Commissioner: Reform bill "a step back overall" for privacy* (2021 May 11), online: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/ nr-c_210511, accessed November 24, 2022.
91. Bill C-26, *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*, 1st Sess, 44th Parl, 2022, 70-71 (First Reading, June 2022), online: https://www.parl.ca/DocumentViewer/en/44-1/bill/C-26/first-reading, accessed November 24, 2022.
92. Defined under *CCSPA*, Schedule 1 as including telecommunications services, interprovincial or international pipeline and power line systems, nuclear energy systems, transportation systems within the legislative authority of Parliament, banking systems and clearing and settlement systems. The Governor in Council also has the authority under s 6(1) to add additional services or systems to Schedule 1.
93. *CCSPA*, s 9.
94. *Ibid.*, ss 15-16.
95. *Ibid.*, ss 17-19.
96. *Ibid.*, ss 20-25.

an incident that interferes with either (a) the continuity or security of a vital service or vital system, or (b) the confidentiality, integrity or availability of the critical cyber system.[106] This leaves the door open to reporting even when there are no specific concerns with threats to an individual's personal information.

The potential punitive consequences for bad actors are high. The *CCSPA* grants the Governor in Council the power to establish penalties for violations of $1 million for individuals or $15 million for any other case.[107]

On June 16, 2022, a mere two days later, Parliament introduced *An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts or the Digital Charter Implementation Act, 2022* (Bill C-27).[108] The overlap between Bill C-27 and Bill C-11 is significant. For example, under Bill C-27:

(a) the CPPA applies to "organizations", again with an identical definition to PIPEDA;[109]
(b) the Data Protection Tribunal will again have authority to impose a maximum penalty for contraventions of the CPPA in the higher of $10,000,000 or 3% of the contravening organization's gross global revenue in its financial year before the one which in the penalty was imposed;[110]
(c) if contravening specific sections of the CPPA, organizations can be found guilty of (i) an indictable offence and liable for a fine not exceeding the higher of $25 million and 5% of the organization's gross global revenue in its preceding financial year, or (ii) an offence punishable on summary conviction and liable to a fine not exceeding the higher of $20 million and 4% of the organization's gross global revenue;[111]

A key distinction between Bills C-27 and C-11 is that Bill C-27 will also allow for monetary penalties for a greater degree of

106. *Ibid.*, s 2.
107. *Ibid.*, s 91.
108. Bill C-27, *An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts or the Digital Charter Implementation Act, 2022*, 1st Sess, 44th Parl, 2022, 7071 (First Reading, June 16, 2022), online: https://www.parl.ca/Document-Viewer/en/44-1/bill/C-27/first-reading, accessed November 24, 2022.
109. *Ibid*, s. 2.
110. *Ibid*, s. 95(4).
111. *Ibid*, s. 128.

contraventions of the CPPA.[112] Notably, Bill C-27 also introduces a private right of action for the individual impacted by a contravention of the CPPA against an organization.[113]

As Bill C-26 passes through the Parliamentary system, organizations that hold any personal data would be wise to keep a careful eye on its development.

CASL

Canada's Anti-Spam Law (*CASL*)[114] includes provisions that have privacy implications, relating to commercial electronic messages. For example, the statute prohibits:

(a) the sending or permitting to be sent to an electronic address a commercial electronic message unless a specific exemption applies or (i) the recipient has consented to receiving it, whether the consent is express or implied; and (ii) the message complies with specific content requirements;[115]
(b) alteration of transmission data in the electronic message so that the message is delivered to a destination other than or in addition to that specified by the sender;[116]
(c) anyone in course of a commercial activity from (i) installing or causing to be installed a computer program on any other person's computer system or (ii) causing an electronic message to be sent from that computer system, unless they receive the express consent of the computer system's owner or an authorized user, or if the person is acting in accordance with a court order;[117] and
(d) sending a commercial electronic message to an electronic address in order to induce or aid any of the above.[118]

CASL as a whole is not enforced by a single body or authority. Rather, the Canadian Radio-Television and Telecommunications Commission (CRTC), the Commissioner of Competition, and the

112. See: *Ibid*, s. 94(1).
113. *Ibid*, s. 107.
114. *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, S.C. 2010, c. 23.
115. *CASL*, s 6.
116. *Ibid.*, s 7(1).
117. *Ibid.*, s 8(1).
118. *Ibid.*, s 9.

Privacy Commissioner must consult with one another (i) to ensure the effective regulation under *CASL*, the *Competition Act*, *PIPEDA* and the *Telecommunications Act* of commercial conduct that discourages the use of electronic means to carry out commercial activities, and (ii) to coordinate activities under those Acts as they relate to the regulation of such conduct.[119]

Monetary penalties under CASL are far more severe than those under *PIPEDA*. The maximum penalty for a single violation is $1 million for individuals and $10 million for "any other person" (*i.e.*, a corporation).[120] However, the penalties the CRTC has imposed to date for violations of *CASL* have remained relatively modest.[121]

CASL has been invoked specifically in the context of cybersecurity threats. In one notable instance, on December 3, 2015, the CRTC announced its first warrant under CASL to take down a command-and-control server in Toronto that was the source of malware threatening computer security.[122]

There have been only a few cybersecurity-related contraventions of CASL investigated to date, but the potential implications for distributors of communications are significant, assuming that the body enforcing the penalty has sufficient evidence to find the contravening organization responsible.[123] Unless and until the

119. Ibid., s 57. The CRTC has the primary enforcement responsibility under CASL. Simplifying the three agencies' enforcement duties: the CRCT deals with non-compliant commercial electronic messages, non-consensual transmission data alteration (e.g., website redirects), and non-consensual computer program installation; the Competition Bureau addresses deceptive marketing practices; the OPC deals with the illegal harvesting of emails addresses. See: https://fightspam-combattrelepourriel.ised-isde.canada.ca/ site/canada-anti-spam-legislation/en/canadas-anti-spam-legislation-resources/canadas-anti-spam-legislation-resources-sub/canadas-anti-spam-legislation-partners-and-links, accessed November 24, 2022. Also see: Canada, "Understanding Canada's anti-spam legislation" (April 1, 2019), online: https://fightspam-combattrelepourriel.ised-isde.canada.ca/site/canada-anti-spam-legislation/en/understand-canadas-anti-spam-legislation/understand-canadas-anti-spam-legislation-sub/understanding-canadas-anti-spam-legislation, accessed November 27, 2022.

120. CASL, s 20(4).

121. Canadian Radio-television and Telecommunications Commission, Enforcement actions, online: https://crtc.gc.ca/eng/ce/actions.htm. For example see, Compliance and Enforcement Decision 2017-368 where the CRTC reconsidered the administrative monetary penalty ordered against a company for its violation of ss 6(1)(a) and 6(2)(c) of CASL. The notice of violation had set out a penalty of $1.1 million, but the CRTC reduced it to $200,000.

122. Government of Canada, "CRTC serves its first-ever warranty under CASL in botnet takedown" (3 December 2015), online: https://www.canada.ca/en/ radio-television-telecommunications/news/2015/12/crtc-serves-its-first-ever-warrant-under-casl-in-botnet-takedown.html.

CCSPA becomes law, *CASL* poses the most significant statutory monetary threat to bad actors in the cybersecurity space. The CRTC is responsible for administering sections 6 to 46 of *CASL*[124] The Competition Bureau and the Privacy Commissioner are similarly responsible for enforcing other parts of *CASL*. However, where an act by an organization is subject to sections 6 to 9 of *CASL*, the Commissioner has the option not to conduct an investigation under *PIPEDA*[125] or discontinue an investigation of a complaint.[126]

Sector-Specific Legislation

Financial Institutions

Outside of general federal privacy statutes, several specific industries are subject to personal information cybersecurity requirements through legislation or other directives.

The *Bank Act*[127] regulates the use and disclosure of personal financial information by federally-regulated financial institutions.[128] The Federal Government also has powers under the *Bank Act*, the *Insurance Companies Act*,[129] and the *Trust and Loan Companies Act*[130] to make regulations requiring financial institutions to (i) establish procedures for the collection, use and disclosure of information about customers, (ii) establish procedures for dealing with complaints about such collection, use and disclosure, (iii) designate officers and employees responsible for implementing information procedures and for receiving and dealing with customer complaints, and (iv) report information related to customer complaints on information matters and the actions taken by institutions to deal with such complaints.[131]

123. See for example: CRTC Compliance and Enforcement Decision CRTC 2022-132, where the CRTC compliance unit had found an online platform to have contravened s. 9 of *CASL* for aiding in a contravention of the Act in the context of malware and spam, but the decision was overturned for lack of evidence.

124. *CASL*, s 62.

125. *PIPEDA*, s. 12(2).

126. *PIPEDA*, s. 12.2(2).

127. SC 1991, c. 46.

128. For example, see: s 410(c).

129. SC 1991, c. 47.

130. SC 1991, c. 45.

131. Barry B. Sookman, *Computer, Internet and Electronic Commerce Law*, (Thomson Reuters: Toronto, ON 2002), ch XI at s. 8:49.

Several private sector authorities have provided non-statutory guidance to address cybersecurity risks for organizations subject to their regulation.

OSFI – the Office of the Superintendent of Financial Institutions– regulates Federally Regulators Financial Institutions (FRFIs), such as banks, most insurance companies and federal pension plans. While OSFI does not have specific regulations for FRFIs regarding cybersecurity, it has issued guidelines and advisories.[132]

2013, OSFI published a guide to assist organizations assess their level of preparedness and implement best cybersecurity practices. This was updated in August 2021, with a focus on 8 categories: governance, identification, defence, detection, response, recovery, learning, and third-party providers.[133] OSFI released separate guidelines on cybersecurity incident reporting around the same time.[134]

In June 2016, OSFI also published a guideline on operational risk management, proposing the following best practices for FRFIs:

(a) operational risk management should be fully integrated within the FRFIs' overall risk management program and appropriately documented;
(b) operational risk management serves to support the overall corporate governance structure of the FRFI;
(c) FRFIs should ensure effective accountability for operational risk management, by using, for instance, a "three lines of defence" approach to separate the key practices of operational risk management and provide adequate independent overview and challenge; and
(d) FRFIs should ensure comprehensive identification and assessment of operational risk through the use of appropriate management tools.[135]

132. Office of the Superintendent of Financial Institutions, Guideline B-10, *Outsourcing of Business Activities, Functions and Processes – with respect to technology-based outsourcing and cybersecurity*, online*:* http://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/cldcmp.aspx, accessed November 24, 2022

133. Office of the Superintendent of Financial Institutions, *Cyber Security Self-Assessment*, online: http://www.osfi-bsif.gc.ca/eng/fi-if/in-ai/pages/ cbrsk.aspx, accessed November 24, 2022.

134. Office of the Superintendent of Financial Institutions, *Technology and Cyber Security Incident Reporting Advisory*, online: https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/adv-prv/Pages/TCSIR.aspx, accessed November 24, 2022.

135. Office of the Superintendent of Financial Institutions, Operational Risk

Finally, in July 2022, OSFI published its Technology and Cyber Risk Management guideline.[136] The guideline is to be read in conjunction with OSFI's earlier guidance, mentioned above. This guideline sets out and explains what OSFI views as the three "key components of sound technology and cyber risk management":[137]

(a) Governance and Risk Management Sets OSFI's expectations for the formal accountability, leadership, organizational structure and framework used to support risk management and oversight of technology and cyber security.
(b) Technology Operations and Resilience Sets OSFI's expectations for management and oversight of risks related to the design, implementation, management and recovery of technology assets and services.
(c) Cyber Security Sets OSFI's expectations for management and oversight of cyber risk.

While not invested with the weight of legislation, OSFI guidelines surely set a standard for security safeguards that FRFIs ought to meet. These will certainly be relevant to any claim against a financial institution for cybersecurity violations.

Telecommunications

Federal telecommunications and radiocommunications legislation predates modern cybersecurity concerns, but is still of potential relevance to them.

The Telecommunications Act grants the CRTC powers to "respond to the economic and social requirements of users of telecommunications services" and to "contribute to the protection of the privacy of persons".[138] The CRTC has implemented several regulations and decisions under the Telecommunications Act touching on privacy protection, such as:

(a) regulating the use of Automatic Dialing-Announcing Devices, automatic equipment capable of storing or producing telephone numbers to be called, and which can be used, alone or in conjunction with other equipment, to convey a

---

Management, online: http://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/ gl-ld/Pages/e21.aspx, accessed November 24, 2022.

136. Office of the Superintendent of Financial Institutions, Guideline B-13, Technology and Cyber Risk Management, online: https://www.osfi-bsif.gc.ca/ Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b13.aspx, accessed November 24, 2022.
137. Ibid.
138. Telecommunications Act, S.C. 1993, c. 38, ss 7(h)-(i).

pre-recorded or synthesized voice message to the number called) for commercial solicitation;[139]

(b) requiring telephone companies offering call display services to also offer customers options to enable them to block the transmission of their personal information;[140]

(c) in the context of a directory database decision, recognizing that protection of subscriber privacy and competition in the provision of directory services was no longer appropriate, as listing information was available from other sources, and subscriber policy was not significantly enhanced, since the most current listing information was not available in machine-readable form;[141] and

(d) outlining rigorous requirements around communications from telemarketers and other unsolicited telecommunica-tions.[142]

The Canadian Security Telecommunications Advisory Committee, established to support Canada's National Strategy for Critical Infrastructure and Canada's Cyber Security Strategy, has also published several guidelines and best practice documents that telecommunications service providers should follow. [143]

139. Telecom Decision 94-10.

140. Telecom Order 94-687.

141. Telecom Decision 95-3.

142. Canadian Radio-television and Telecommunications Commission Unsolicited Telecommunications Rules.

143. Canadian Telecommunications Cyber Protection, "Security Best Practice Policy for Canadian Telecommunications Service Providers (CTSPs)" (January 2020) online: https://www.ic.gc.ca/eic/site/smt-gst.nsf/vwapj/CSTAC_CCCSTsecuritybestpractices2020_01EN.pdf/$FILE/CSTAC_CCCSTsecuritybestpractices2020_01EN.pdf, accessed November 24, 2022; Canadian Telecommunications Cyber Protection, "Critical Infrastructure Protection Standard for Canadian Telecommunications Service Providers (CTSPs)" (January 2020), online: https://www.ic.gc.ca/eic/site/ smt-g st. nsf/vwapj / C STAC_C CC STcritic alInfra structurePr otecti o-n2020_01EN.pdf/$FILE/CSTAC_CCCSTcriticalInfrastructureProtection2020_01EN.pdf, accessed November 24, 2022; Canadian Telecommunications Cyber Protection, "Network Security Monitoring and Detection Standard for Canadian Telecommunications Service Providers (CTSPs)" (January 2020), online: https://www.ic.gc.ca/eic/site/smt-gst.nsf/vwapj/CSTAC_CCCSTNetworkSecurityMonitoringandDetection2020_01EN.pdf/$FILE/CSTAC_CCCSTNetworkSecurityMonitoringandDetection2020_01EN.pdf, accessed November 24, 2022; Security Incident Response Standard for CTSPs; Canadian Telecommunications Cyber Protection, "Information Sharing, Reporting and Privacy Standard for Canadian Telecommunications

The Radiocommunication Act,[144] although related to a now antiquated form of technology, also contains provisions that could apply to cybersecurity and data protection.[145]

Securities

The securities and investment sectors have unsurprisingly issued directives to address concerns with cybersecurity.

The Canadian Securities Administrators (CSA) a collective of Canada's provincial and territorial securities regulators whose objective is to improve, coordinate, and harmonize regulation of Canadian capital markets released a staff notice on cybersecurity in September 2013.[146] The CSA emphasized the need for issuers, registrants, and regulated entities in the securities market to be aware of the challenges of cybercrime, and take appropriate measures to safeguard themselves, clients, and stakeholders. The CSA explicitly emphasized DDoS attacks and advanced persistent threats as two major types of cyber threats increasing in frequency and sophistication.

In September 2016, the CSA updated its notice, reiterating that, once market participants determine that cyber risk is a material risk, they should provide detailed and entity-specific risk disclosure, and avoid general boilerplate disclosure.[147] The CSA also advised that cyberattack remediation plans should address how the materiality of a cyberattack would be assessed, to determine what needs to be disclosed in accordance with applicable securities laws, and when or how to make disclosure. It also reminded registrants to continue

Service Providers (CTSPs)" (March 2020), online: https://www.ic.gc.ca/eic/site/smt-gst.nsf/vwapj/CSTAC_CCCSTinformationSharingAndReporting2020_01EN.pdf/$FILE/CSTAC_CCCSTinformationSharingAndReporting2020_01EN.pdf, accessed November 24, 2022.

144. RSC 1985, c. R-2.

145. For example, see s 9(1)(c), which prohibits the decoding of an encrypted subscription program signal or encrypted network feeds, otherwise under and in accordance with authorization from the lawful distributor of the signal or feed or operating a radio apparatus, so as to receive an encrypted subscription programming signal or encrypted network feed that has been decoded in contravention of the Act. This would apply to, for example, the decoding of satellite signals, unless authorization from a lawful Canadian distributor has been received.

146. Ontario Securities Commission, CSA Staff Notice 11-326 Cyber Security, online: https://www.osc.ca/en/securities-law/instruments-rules-policies/1/11-326/csa-staff-notice-11-326-cyber-security, accessed November 24, 2022.

147. Ontario Securities Commission, CSA Staff Notice 11-332 Cyber Security, online: https://www.osc.ca/sites/default/files/pdfs/irps/sn_20160927_11-332-cyber-security.pdf, accessed November 24, 2022.

developing, implementing, and updating their approach to cyber security hygiene and management.

In the ensuing years, the CSA has continued to issue directives that touch on other cybersecurity risks:

(a) on October 19, 2017, the CSA issued a notice to inform firms on cybersecurity risks associated with social media use;[148] and

(b) on October 18, 2018, the CSA issued a notice to inform market participants about the CSA's coordination process to address market disruption, including those involving a larger-scale cybersecurity incident (with reference to prior no-tices).[149]

Other organizations in the securities space have issued similar directives. For example, the Investment Industry Regulatory Organisation of Canada (IIROC) has published substantial directives for dealer members on protecting themselves and clients from cyberattacks. These directives deal with (i) cybersecurity best practices, (ii) cyber incident management planning, (iii) cyber program governance (with a focus on assessing and managing technology risk), and (iv) the fundamentals of technology risk management.[150]

Similarly, the Mutual Fund Dealers Association of Canada (MFDA) has issued bulletins for its members pertaining to cybersecurity, relating to: (i) understandings of cybersecurity generally,[151] (ii) development of cybersecurity assessment programs[152] (iii) understandings of cybercriminals' conduct during the COVID-19 pandemic,[153] (iv) security safeguards while working

148. Ontario Securities Commission, CSA Staff Notice 33-321: *Cyber Security and Social Media*, online: https://www.osc.ca/sites/default/files/pdfs/irps/csa_20171019_33-321_cyber-security-and-social-media.pdf, accessed November 24, 2022.

149. Ontario Securities Commission, CSA Staff Notice 11-338: CSA Market Disruption Coordination Plan, online: https://www.osc.ca/sites/default/files/pdfs/irps/csa_20181018_11-338_market-disruption-coordination-plan.pdf, accessed November 24, 2022.

150. IIROC, Guides and Resources: https://www.iiroc.ca/sections/members/cybersecurity-technology/guides-and-resources, accessed November 24, 2022.

151. MFDA, Bulletin 0690-C: Cybersecurity, online: https://mfda.ca/bulletin/bulletin0690-c/, accessed November 24, 2022.

152. MFDA, Bulletin 0763-C: Cybersecurity Assessment Program, online: https://mfda.ca/bulletin/bulletin0763-c/, , accessed November 24, 2022.

153. MFDA, Bulletin 0816-M: Cybercriminals Currently Exploiting the COVID-19 Pandemic, online: https://mfda.ca/bulletin/bulletin0816-m/, accessed November 24, 2022.

from home,[154] (v) developing cybersecurity assessment programs.[155] and (vi) the legal aspects of cybersecurity.[156]

As with OSFI's guidelines for FRFIs, the securities-related guidelines are not statutory, but set a standard that will be relevant to claims against industry members for cybersecurity violations.

ii. Public Sector

Privacy Act

Statutory Framework

In the federal public sector, the primary piece of legislation governing public actors is the Privacy Act, which regulates the collection, use and disclosure of personal information held by federal institutions.[157]

Federal institutions include any department or ministry of the Government of Canada, any government body in the lengthy list of specific federal government institutions under the Privacy Act, and Crown corporations and wholly owned subsidiaries of Crown corporations.[158]

The statute applies to personal information, broadly defined as "information about an identifiable individual that is recorded in any form".[159] Government institutions may collect personal information directly from an individual, but must ensure that it is accurate, up-to-date, and complete.[160] These institutions cannot use this information for a purpose other than, or inconsistent with, the

154. MFDA, Bulletin 0821-M: MFDA Webinar: The Importance of Working Securely From Home, online: https://mfda.ca/bulletin/bulletin0821-m/, accessed November 24, 2022.

155. MFDA Bulletin 0830-M: MFDA Technology Webinar Series: Cybersecurity Assessment Program, online: https://mfda.ca/bulletin/bulletin0830-m/, accessed November 24, 2022.

156. MFDA, Bulletin 0854-M: MFDA Technology Webinar Series: Legal Aspects of Cybersecurity and Cyber-Risk Management, online: https://mfda.ca/bulletin/bulletin0854-m/, accessed November 24, 2022.

157. Office of the Privacy Commissioner of Canada, Summary of privacy laws in Canada. online: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/, accessed November 24, 2022.

158. Privacy Act, Schedule.

159. Privacy Act, s. 3. This definition includes information with respect to one's race, national or ethnic origin, colour, religion, age, marital status, education, criminal history, employment history, medical history, address, fingerprints, views or opinions or discretionary benefit of a financial nature.

160. Privacy Act, ss 4-6.

one for which it was collected, without the individual's consent.[161] The test for such a purpose is a "sufficiently direct connection".[162]

A government institution may not disclose personal information, except where (i) the subject individual consents, (ii) the information is publicly accessible, or (iii) disclosure is in accordance with the purposes set out under the Privacy Act, i.e., enforcing a law of Canada or carrying out an investigation.[163] If the institution can meet the onus of demonstrating that the personal information is "publicly available" and accessible to citizens at large (such as through the Internet), then the prohibition against disclosure will not apply.[164]

The *Privacy Act* works in conjunction with the Federal *Access to Information Act* to create a seamless code.[165] As Justice La Forest noted in *Dagg v. Canada (Minister of Finance)*, in interpreting these statutes, "privacy is paramount."[166]

161. *Privacy Act*, ss 7.

162. *PIPSC v. Canada (Revenue Agency)*, 2014 SCC 13, (*sub nom.* Bernard v. Canada (Attorney General)) [20141 1 S.C.R. 227, 367 D.L.R. (4th) 631 (S.C.C.); *O'Grady v. Canada (Attorney General)*, 2017 FC 167, 23 Admin. L.R. (6th) 261, 276 A.C.W.S. (3d) 78 (F.C.), at para. 69; *Prairie North Health Region and CUPE, Local 5111 (Employee Name Tags), Re* (2015), 264 L.A.C. (4th) 16, 2015 CarswellSask 768, [20151 S.L.A.A. No. 17 (Sask. Arb.), at para. 136.

163. *Privacy Act*, ss 7(a)-(b), 8(1)-(2). Other purposes include: (a) for which the information was obtained and compiled; (b) the purpose in accordance with any Act of Parliament or regulation; (c) for legal proceedings involving the Crown of Government of Canada; (d) for an investigative body specified in the regulations for the purpose of enforcing a law of Canada or a province or carry out an investigation; and (e) where a head of an institution opines that the public interest and the benefit to the subject of the information outweighs concerns with invasion of privacy; *Access to Information Act*, RSC 1985, c. A-1, s 19(1)-(2).

164. *Privacy Act*, s 69(2); *Martin v. Canada (Minister of Health)*, 2016 FC 796, 269 A.C.W.S. (3d) 405, 2016 CarswellNat 3620 (F.C.), at paras. 53-57; *LukA¨cs v. Canadian Transportation Agency*, 2015 FCA 140, 386 D.L.R. (4th) 163, 88 Admin. L.R. (5th) 24 (F.C.A.), at para. 69; *Husky Oil Operations Ltd. v. Canada-Newfoundland and Labrador Offshore Petroleum Board*, 2016 FC 117, 263 A.C.W.S. (3d) 279, 2016 CarswellNat 187 (F.C.) at paras. 13-15, affirmed *Husky Oil Operations Limited v. Canada-Newfoundland and Labrador Offshore Petroleum Board*, 2018 FCA 10, 418 D.L.R. (4th) 112, 287 A.C.W.S. (3d) 569 (F.C.A.).

165. *H.J. Heinz Co. of Canada Ltd. v. Canada (Attorney General)*, 2006 SCC 13, [20061 1 S.C.R. 441, 266 D.L.R. (4th) 675 (S.C.C.), at para. 2, citing *Canada (Information Commissioner) v. Royal Canadian Mounted Police Commissioner*, 2003 SCC 8, (*sub nom.* Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police)) [20031 1 S.C.R. 66, 224 D.L.R. (4th) 1 (S.C.C.), at para. 22.

Available Statutory Remedies

The *Privacy Act* offers a comprehensive regime for investigating alleged violations of the statute, but there are no civil remedies for violations of the *Privacy Act*.[167]

Rather, the Privacy Commissioner of Canada receives and investigates all complaints under the *Privacy Act* from individuals regarding (i) improper use or disclosure of information by a government institution, or (ii) improper refusal to provide access to information.[168]

The Commissioner has broad investigative powers, including the power to (i) enter an institution's premises, (ii) examine information under the institution's control,[169] and (iii) (somewhat contentiously) inspect and disclose solicitor-client privileged documents if necessary.[170] If the Commissioner determines that a complaint was well-founded, they report the results of the investigation and recommend next steps to the head of the institution in control of that information. If the head of the institution refuses to follow that recommendation, they must provide an explanation.[171]

Similarly, if unsatisfied with an institution's refusal to provide access to information or with the Commissioner's investigative report, an individual may apply to the Federal Court for judicial

---

166. *Dagg v. Canada (Minister of Finance)*, [19971 2 S.C.R. 403, 148 D.L.R. (4th) 385, 46 Admin. L.R. (2d) 155 (S.C.C.), at para. 48.

167. See for example: *Kim v. Canada*, 2017 FC 848, 284 A.C.W.S. (3d) 417, 2017 CarswellNat 5222 (F.C.), at para. 24, where the Federal Court of Canada used to recognize an independent tort of statutory breach in the context of a violation of the provisions of the *Privacy Act*.

168. *Privacy Act*, s 29(1).

169. *Privacy Act*, ss 34-35.

170. *Canada (Information Commissioner) v. Canada (Minister of Environment)* (2000), 187 D.L.R. (4th) 127, 21 Admin. L.R. (3d) 1, (*sub nom.* Canada (Minister of the Environment) v. Canada (Information Commissioner)) 256 N.R. 162 (Fed. C.A.) at paras. 11, 21, leave to appeal refused (2000), (*sub nom.* Canada (Minister of the Environment) v. Information Commissioner (Can.)) 266 N.R. 198 (note), 2000 CarswellNat 2725, 2000 CarswellNat 2726 (S.C.C.). However, some courts have ruled that there was no intention for commissioners' powers to extend to solicitor-client privileged documents. See for example: *Blood Tribe Department of Health v. Canada (Privacy Commissioner)*, 2006 FCA 334, 274 D.L.R. (4th) 665, 53 C.P.R. (4th) 273 (F.C.A.) at para. 29, affirmed 2008 SCC 44, [20081 2 S.C.R. 574, 2008 CarswellNat 2244 (S.C.C.); *A.T.A. v. Alberta (Information & Privacy Commissioner)*, 2011 SCC 61, (*sub nom.* Alberta (Information & Privacy Commissioner) v. Alberta Teachers' Association) [20111 3 S.C.R. 654, 339 D.L.R. (4th) 428 (S.C.C.), at para. 49.

171. *Privacy Act*, s 35(1).

review.[172] The standard of review for a government institution's refusal to disclose records is reasonableness.[173]

In *Thomas v. Canada (Public Safety and Emergency Preparedness)*,[174] the Federal Court referenced *Vavilov* in dismissing an application for judicial review of a decision of a Canada Border Services Agency officer. In challenging the officer's decision to charge him with breaches of the *Customs Act* and *Export and Support of Rough Diamonds Act*, the Applicant sought a confidentiality order, relying on protections from disclosure under section 45 of the *Privacy Act*. In dismissing the application, Justice Pentney noted that, following Vavilov, reasonableness is the presumptive standard in reviewing the officer's decision, which the Court held was reasonableness.

Other Public Directives

Other government bodies have nevertheless provided additional guidance on cybersecurity. For example, Public Safety Canada, the department responsible for ensuring coordination across all federal departments and agencies for national security, has put in place specific guidelines, including:

(a) the National Cyber Security Strategy;[175]
(b) the National Cyber Security Action Plan (2019-2024);[176] and
(c) the Cyber Security Cooperation Program.[177]

172. Ibid., s 41. See for example: *Doyle v. Canada (Minister of Human Resources Development)*, 2011 FC 471, 200 A.C.W.S. (3d) 1196, 2011 CarswellNat 1228 (F.C.), at paras. 21-24; *Clancy v. Canada (Minister of Health)*, 2002 FCT 1331, 119 A.C.W.S. (3d) 359, 2002 CarswellNat 3717 (Fed. T.D.), at paras. 10-12.

173. *Vavilov*, at para 10. See for example: *Thomas v. Canada (Public Safety and Emergency Preparedness)*, 2020 FC 290, 75 Admin. L.R. (6th) 25, 316 A.C.W.S. (3d) 458 (F.C.) for application of the *Vavilov* standard of review in the context of the *Privacy Act*.

174. *Thomas v. Canada (Public Safety and Emergency Preparedness)*, 2020 FC 290, 75 Admin. L.R. (6th) 25, 316 A.C.W.S. (3d) 458 (F.C.), at para. 29.

175. Canada, Public Safety Canada, "National Cybersecurity Strategy" (2019 May 28) online: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx, accessed November 24, 2022.

176. Canada, Public Safety Canada, "National Cyber Security Action Plan (2019-2024)" (2020 April 15), online: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/index-en.aspx, accessed November 24, 2022.

177. Canada, Public Safety Canada, "Cyber Security Cooperation Program" (2020 December 15), online: https://www.publicsafety.gc.ca/cnt/ntnl-scrt/ cbr-scrt/cprtn-prgrm/index-en.aspx, accessed November 24, 2022.

In conjunction with Public Safety, the Communication Securities Establishment (the technical authority for cybersecurity and information assurance) is mandated under s. 76 of the *Communications Security Establishment Act*[178] to acquire, use and analyze information from the global information infrastructure, or from other sources, to provide advice, guidance, and services to protect electronic information and information infrastructures.

Similarly, under s. 19 of the *Security of Information Act*,[179] it is an offence for any person to fraudulently, and without colour of right, communicate a trade secret to another person, or obtain, retain, alter, or destroy a trade secret to the detriment of Canada's economic interests, international relations, or national defence/national security. This carries a maximum penalty of 10 years' imprisonment.

Although not as far-reaching as private sector laws, federal statutes do provide an extensive scheme to hold federal public actors accountable for privacy and cybersecurity transgressions. However, in the absence of civil remedies under the *Privacy Act*, the uses of litigation are limited.

iii. Criminal

The *Criminal Code* of Canada has no cybercrime provision, but it does include specific offences encompassing cybersecurity.

Different offences under the *Criminal Code* can involve data, [180] theft,[181] extortion,[182] mischief,[183] forgery,[184] conveyance of false messages,[185] falsification of books,[186] false pretence,[187] identity fraud,[188] and intimidation.[189] There are also offences tailored to personal information and data, or that have been applied for such purposes. These include:

(a) fraud under section 380(1) where individuals have been involved in email phishing scams;[190]

---

178. *Communications Security Establishment Act*, S.C. 2019, c. 13.
179. *Security of Information Act*, R.S.C. 1985, c. O-5.
180. Sookman, *supra* at s 7.1.
181. *Criminal Code*, R.S.C., 1985, c. C-46, s 322.
182. *Ibid.*, s 346.
183. *Ibid.*, s 430.
184. *Ibid.*, s 366.
185. *Ibid.*, s 372.
186. *Ibid.*, s 397.
187. *Ibid.*, ss 361-362.
188. *Ibid.*, s 403.
189. *Ibid.*, s 423.
190. *R. v. Usifoh*, 2017 ONCJ 451, 141 W.C.B. (2d) 306, 2017 CarswellOnt 10708

(b) willfully using a device to intercept a private communication without the express or implied consent of the originators or intended recipient,[191] which has obvious implications for cybercrime;
(c) unlawful interception under section 183 (defined as including to "listen to, record or acquire a communication or acquire the substance, meaning or purport thereof") which has been found to include the seizure of text messages that are stored on a telecommunication provider's computer;[192]
(d) under section 342.1, interception of any function of a computer system fraudulently and without colour of right;[193]
(e) where a person commits mischief to destroy or alter computer data, render computer data meaningless, useless or ineffective, obstruct, interrupt or interfere with the lawful use of computer data, or obstruct, interrupt or interfere with a person's lawful use of computer data who is entitled to access it.[194] This has been specifically applied in the context of cybersecurity, where an accused was convicted under subsection 430(5) after pleading guilty to "hacking" after obtaining 400 credit card numbers and other personal data and accessing the internet 48 times using false identification;[195]
(f) obstructing, interrupting, or interfering with the lawful use of computer data or deny access to computer data to a person who is entitled to access it, with a maximum penalty of 10 years' imprisonment;[196]
(g) unlawfully selling or offering for sale a device designed or adapted primarily to commit cybercrime, knowing that the device is prohibited under sections 342.1 or 430';[197]
(h) committing identity theft and identity fraud.[198] Convictions have included for identity fraud (and unauthorized access to

(Ont. C.J.), affirmed 2019 ONCA 814, 158 W.C.B. (2d) 389, 2019 CarswellOnt 16110 (Ont. C.A.).

191. *Criminal Code of Canada*, s 184.

192. *R. v. Telus Communications Co.*, 2013 SCC 16, (*sub nom.* R. v. TELUS Communications Co.) [20131 2 S.C.R. 3, 356 D.L.R. (4th) 195 (S.C.C.); *Criminal Code*, ss. 183-184, 193.

193. This crime involves five essential elements, see: *R. v. Senior*, 2021 ONSC 2729, 172 W.C.B. (2d) 321, 2021 CarswellOnt 5857 (Ont. S.C.J.), at para. 304.

194. *Criminal Code*, s 430.

195. *R. v. Geller* (2003), 56 W.C.B. (2d) 667, 2003 CarswellOnt 687, [20031 O.J. No. 357 (Ont. S.C.J.).

196. *Criminal Code*, s 430(1.1)

197. *Ibid*, s 342.2.

198. *Ibid*, ss 402.2, 403.

use of a computer) after accessing Facebook accounts of minors and personating those minors' friends to lure them into child pornography;[199] and

(i) committing an indictable offence under the Code or any other Act of Parliament for the benefit of, at the direction of or in association with a terrorist group.[200] The definition of "terrorist activity" under section 83.01 includes an act that causes interference or serious disruption of an essential service, facility, or system, whether public or private, other than as a result of non-violent advocacy, protest, dissent or stoppage of work. This can include cyberterrorism.

However, the *Criminal Code* has its limits when it comes to privacy and cybersecurity offences. The identity of the hacker or cyberattacker must be known. Also, non-tangible property, such as data or information, is not considered property. So, with the exception of identity theft, data exfiltrated by hacking cannot be "stolen" under the theft provisions of the *Code*.[201]

C. Provincial

i. BC, Alberta, and Québec PIPA

As noted, the only Canadian provinces to implement general private sector statutes like *PIPEDA* have been Alberta, BC, and Québec.

Each of these pieces of legislation have substantial similarities to their federal counterparts, including enforcement protocols.

BC PIPA

In BC, with certain exceptions, *PIPA* applies to the collection, use and disclosure of personal information by "organizations", defined as including persons, unincorporated associations, trade unions, trusts and not-for-profit organizations.[202]

199. R. v. Mackie, 2014 ABCA 221, 626 W.A.C. 1, 588 A.R. 1 (Alta. C.A.).
200. Criminal Code, s 83.2.
201. R. v. Stewart, [1988] 1 S.C.R. 963, 50 D.L.R. (4th) 1, 41 C.C.C. (3d) 481 (S.C.C.); *ORBCOMM Inc. v. Randy Taylor Professional Corp.*, 2017 ONSC 2308, 278 A.C.W.S. (3d) 824, 2017 CarswellOnt 5148 (Ont. S.C.J.) at para. 26, additional reasons 2017 ONSC 4488, 281 A.C.W.S. (3d) 481, 2017 CarswellOnt 11507 (Ont. S.C.J.).
202. Personal Information Protection Act, SBC c 63 (BC *PIPA*), s 1.

Under the statute, organizations are allowed to collect, use and disclose personal information about an individual only with the individual's knowledge and consent and only for the purposes that a reasonable person would consider appropriate in the circumstances.[203]

Organizations must take positive steps to develop and follow policies and practices that are necessary for the organization to meet their obligations under PIPA, develop a process to respond to complaints that may arise respecting PIPA's application, and make these policies and practices (along with the complaint process) available upon request.[204]

Unique to PIPA, there have now been multiple decisions holding Canada's federal political parties to be "organizations" under PIPA and, as such, within the purview of PIPA. The practical implications for the political parties have yet to be seen.[205]

PIPA also applies to employee personal information, i.e., information about an individual collected, used, or disclosed solely for the purposes reasonably required to establish, manage, or terminate the employment relationship between the organization and the individual. This also permits an employer to collect, use and disclose employee personal information without employee consent, reasonably, for the purpose of establishing, managing, or terminating an employment relationship. Here, the employer must, in advance, notify the employee that it will be collecting, using, and disclosing employee personal information, and identify the purposes for which the information will be collected, used, and disclosed.[206]

Alberta PIPA

Alberta PIPA is substantially similar to BC PIPA, having come into force on the same day.

Alberta PIPA applies to the collection, use and disclosure of information by "organizations", which includes corporations, unincorporated associations, trade unions, partnerships and individuals acting in a commercial capacity, but not an individual acting in a personal or domestic capacity.[207]

The statute also includes similar requirements as BC PIPA regarding the implementation by organizations of policies and procedures to meet their obligations.[208]

203. BC PIPA, ss 6-8.
204. BC PIPA, s 5.
205. See discussions above.
206. BC PIPA, s 13.
207. Personal Information Protection Act, SA 2003, c. P-65 (Alta PIPA), s. 1.

Both BC and Alberta *PIPA* include four conditions for an organization to collect, use and disclose personal information:

(a) the organization provides the individual with notice, in a form that the individual can reasonably be considered to understand, that it intends to collect, use or disclose the individual's personal information for these purposes;
(b) the organization gives the individual a reasonable opportunity to decline the proposed collection, use or disclosure within a reasonable time;
(c) the individual does not decline, within the time under (b), the proposed collection, use or disclosure; and
(d) the proposed collection, use or disclosure of personal information is reasonable having regard to the sensitivity of the personal information in the circumstances.[209]

Under Alberta *PIPA* and BC *PIPA*, the Offices of the Information and Privacy Commissioner have similar investigative powers as the Federal Commissioner under *PIPEDA*.[210] Under both statutes, the Commissioner may also elevate a complaint by an individual to a formal inquiry.[211]

Both statutes also grant individuals a cause of action against an organization for actual harm[212] or loss or injury[213] as result of the organization's contravention of the statute. This differs from *PIPEDA*, which invests the Commissioner with the power to award damages. The Alberta OIPC has noted expressly that damages should only be sought through the Courts, and not their office.[214] However, to date, awards of damages from the Superior Courts under these statutes have been limited.

Québec PIPA

Québec's counterpart legislation governs the protection of personal information (defined as any information relating to a natural person and allowing them to be identified) and its collection, holding, use or communication.[215]

208. Alta *PIPA*, s 6.
209. BC *PIPA*, s 8(3); Alta *PIPA*, s 8(3).
210. BC *PIPA*, ss 36-44; Alta *PIPA*, ss 36-44.
211. BC *PIPA*, s 50; Alta *PIPA*, s 50.
212. BC *PIPA*, s 57.
213. Alta *PIPA*, s 60.
214. *Anthony Clark International Insurance Brokers Ltd., Re*, 2010 CarswellAlta 2952 (Alta. I.P.C.), at paras. 22-23.

Québec *PIPA* also includes provisions relating to the retention, use and non-communication of information. Specifically, provisions requiring the use of appropriate security,[216] files being up-to-date and accurate when used to make a decision in relation to a person,[217] and no information in a file being used otherwise than in accordance with the object of the file without the consent of the person concerned.[218]

The act also prohibits a person from communicating to a third person personal information contained in a file, or from using it for purposes not relevant to the object of the file, without the data subject's consent, unless expressly permitted by Québec PIPA.[219] Consent requirements are also extremely specific, and must be "manifest, free, and enlightened" and "be given for specific purposes".[220]

Regarding enforcement, Québec *PIPA* includes specific provisions allowing the Québec privacy commissioner to appoint inspectors or conduct inquiries into matters relating to the protection of personal information,[221] and ultimately issue reports or directions.[222]

Although Québec *PIPA* includes provisions for fines as penalties for contravening the act,[223] it offers no right to damages in such circumstances.

Revising Québec PIPA: Bill 64

Québec has taken a bold step in modernizing its privacy legislation with Bill 64,[224] which was assented to on September 22, 2021. It comes into force on September 22, 2023, with some exceptions.[225]

215. *Act Respecting the Protection of Personal Information in the Private Sector*, P-39.1 (Que *PIPA*), ss 1-2.
216. Que *PIPA*, s. 10.
217. Que *PIPA*, s. 11.
218. Que *PIPA*, s. 12.
219. Que *PIPA*, s. 13.
220. Que *PIPA*, s. 14.
221. Que *PIPA*, ss 80.2-81.
222. Que *PIPA*, ss 83-89.
223. Que *PIPA*, ss 91-93.
224. Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information*, 1st Sess, 42nd Parl, Québec, c 25 (as assented to 22 September 2021) (Bill 64).
225. Québec, National Assembly of Québec, "Projet de loi nº 64", online: http://assnat.qc.ca/fr/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html, accessed November 24, 2022.

Entitled An Act to modernise legislative provisions as regards the protection of personal information, the bill introduces into Canadian law GDPR-inspired principles. It also amends Québec *PIPA* generally.

Bill 64 requires organizations to establish data governance and management practices and policies. They must have updated policy guidelines for staff and service providers that reflect Bill 64's standards. They must de-index or transfer personal information, if asked.

Organizations will have greater cyber-reporting obligations. These include notifying individuals if a confidentiality incident poses a "risk of serious injury",[226] and taking reasonable measures to prevent, and reduce the risk or injury from, new incidents.

New transparency and consent standards will require end-users' consent to be clear, free and informed, and given for specific purposes – a higher standard than the one under *PIPEDA*.[227]

Penalties are robust. The monetary administrative penalty is $50,000 for natural persons. In all other cases, the maximum is $10 million or 2% of worldwide turnover for the preceding fiscal year, whichever is greater.[228]

Although Bill 64 is provincial legislation, its effect will likely be significant in two ways: (1) by imposing changes that organizations conducting business in Québec may adopt outside the province, and (2) by influencing on legislators and policymakers Canada-wide.

ii. More Provincial Privacy Legislation on the Horizon

In June 2021, the Ontario government released the White Paper *Modernizing Privacy in Ontario*.[229] The document proposes several updated provisions for a new provincial statute.

The White Paper suggests implementing stricter requirements than those under the federal Bill C-11. Although not necessarily a priority for the current Ontario government, the White Paper outlines GDPR-inspired rights, enforcement, and penalties, including for employee personal information not subject to Canadian privacy laws at the moment.

---

226. Bill 64, s 3.5.
227. Bill 64, s 14.
228. Bill 64, s 90.12.
229. Ontario, "Modernizing Privacy in Ontario: Empowering Ontarians and Enabling the Digital Economy" *White Paper* (17 June 2021), online: https://www.ontariocanada.com/registry/showAttachment.do?postingId=37468&attachmentId=49462, accessed November 24, 2022.

The Information and Privacy Commissioner of Ontario has issued a response to the White Paper.[230] The response offers a multitude of recommendations and comments, including empowering the IPC to offer compliance support tools, such as advisory services, sectoral codes of practice and certification programs, with a special focus on "agile" regulation of SMEs. The response also calls for penalty powers that include "*consideration of any regulatory action already taken by other jurisdictions as a possible mitigating factor, ensuring a harmonized, fair and proportionate approach*."

It remains to be seen how the White Paper will inform and impact legislation governing privacy and cybersecurity in Ontario and elsewhere in Canada.

iii. Health

Statutory Overview

Every province and territory in Canada (except Prince Edward Island) has legislation governing personal health information that is collected, used or disclosed by health information custodians.[231]

This section is not an exhaustive study on Canadian health privacy laws in Canada. That could be its own paper. We will use Ontario as an example, keeping in mind that our focus is on cybersecurity and litigation.

In Ontario, the *Personal Health Information Protection Act* (PHIPA) establishes rules for the collection, use and disclosure of personal health information. It also grants individuals a right to access, correct, or amend their personal health information.

230. Ontario, Information and Privacy Commissioner of Ontario, *IPC Comments on the Ontario Government's White Paper on Modernizing Privacy in Ontario* (September 2021), online: https://www.ipc.on.ca/wp-content/uploads/2021/09/2021-09-03-ipc-comments-on-gov-white-paper_modernizing-privacy-in-ontario.pdf.

231. *Personal Health Information Act*, 2004, *SO 2004, c 3, Sched. A*, s 1; *E-Health (Personal Health Information Access and Protection of Privacy) Act*, SBC 2008, c 38; *Health Information Act*, RSA 2000, c H-5; *Health Information Protection Act*, SS 1999, ch H-0.021; *Personal Health Information Protection Act*, CCSM c P33.5; *Personal Health Information Act*, SNS 2010, c 41; *Personal Health Information Act*, SNL 2008, c P-7.01; *Personal Health Information Privacy and Access Act*, SNB 2990, c P-7.05; *Health Information Act*, RSPEI 1988, c H-1.41; *Health Information Privacy and Management Act*, SY 2013, c 16; *Health Information Act*, SNWT 2014, c 2.

PHIPA applies to "personal health information", which it defines as identifying information about an individual in oral or recorded form.[232] It then defines "identifying information" as information that identifies an individual, or for which it is reasonably foreseeable in the circumstances that it could be utilized to identify the individual.[233] PHIPA also applies to identifying information about an individual that is not personal health information in its own right, but part of a record that contains other such personal health information.[234]

PHIPA applies to the collection, use and disclosure of personal health information that is held by "health information custodians" who operate in the public and private sectors, including regulated health professionals and hospitals.[235] These custodians may appoint an agent, if they are unwilling to assume such responsibilities.[236] The agent will then be responsible for responding to inquiries about the custodian's information practices, and requests for access to or correction of personal health information. The agent must also receive complaints related to alleged contraventions of the statute.[237]

Health information custodians are responsible for ensuring the personal health information in their possession is retained, transferred, and disposed of in a secure manner, as prescribed by PHIPA's regulations.[238] They must also retain personal health information subject to a request for access for as long as necessary to allow an individual to exhaust their remedies under PHIPA.[239]

Threat actors are somewhat targeted by the health information statutes. For example, Alberta's Health Information Act targets hacking (and similar wrongdoing) by making it an offence to collect, gain or attempt to gain access to personal health information in contravention of the Act.[240]

Remedies

The remedies under each provincial health statute are distinct, with some overlap.

232. PHIPA, s 4.
233. Ibid., s 4(2).
234. Ibid., s 4(3).
235. Ibid., ss 2-3.
236. Ibid., s 15(2).
237. Ibid., s 15(3).
238. PHIPA, s 13(1).
239. PHIPA, s 13(2).
240. Health Information Act, RSA 2000, c. H-5, s. 107.

Ontario residents denied their rights under *PHIPA* may complain to the Information and Privacy Commissioner of Ontario, and ultimately sue for damages for harm they have suffered.[241]

An individual who has been refused access to, or denied a request for the correction of, their personal health information, or has not received a response from the health information custodian, may request that the Ontario Commissioner conduct an investigation.[242]

Upon receiving a complaint, the Commissioner may authorize a mediator to review the complaint and try to have the parties settle.[243] If mediation fails, then the Commissioner will review the matter and make an order or provide comments and recommendations to the relevant parties.[244] If the Commissioner's decision is a final order, it may be filed with the Ontario Superior Court of Justice, rendering it effective and enforceable as a judgment or order of the Court.[245] A party affected by the Commissioner's order may also appeal to the Divisional Court on a question of law.[246] When making an order, the Commissioner has the authority to require a person to pay an administrative penalty, which must be made for the purposes of encouraging compliance with *PHIPA* and its regulations, and preventing a person from deriving an economic benefit as a result of their contravention of the Act or its regulations.[247]

The Commissioner may also refer complaints to the Attorney General for prosecution. This can give rise to fines of at least $25,000.[248]

Where the Commissioner has made a final order under *PHIPA* without a further right of appeal, *PHIPA* grants individuals the right to sue for damages in the Ontario Superior Court of Justice, for actual harm suffered as a result of the contravention of the Act.[249]

PHIPA does not exclude other remedies for privacy breaches. In *Hopkins v. Kay*, the Court of Appeal for Ontario held that PHIPA does not oust the jurisdiction of the Ontario Superior Court to

241. *PHIPA*, ss 56-65.
242. *Ibid.*, s 56(3).
243. *Ibid.*, s 57(1).
244. *Ibid.*, s 57(3), 61(3).
245. *Ibid.*, ss 63-64.
246. *Ibid.*, ss 62(1), 64(4).
247. *Ibid.*, s. 61.1.
248. Ontario, Information and Privacy Commissioner of Ontario, "Health Record Snooping Case Prosecuted in Goderich" (March 16, 2017), online: https://www.ipc.on.ca/newsrelease/health-record-snooping-case-prosecuted-in-goderich/, accessed November 24, 2022.
249. *PHIPA*, s 65.

entertain common law claims for invasion of privacy relating to patient records.[250]

Public Sector: Provincial and Municipal

Each province and territory also has provincial counterparts to the federal *Privacy Act* which specifically governs the protection of personal information held by provincial and municipal government bodies and institutions.[251]

The provincial acts are intended to protect individual privacy and govern the collection, use, retention, and disclosure of personal information by provincial government institutions. They aim to ensure government institutions use personal information only to the extent necessary for legitimate operations, ensure individuals obtain access to personal information (in most circumstances), and substantially restrict third party access to personal information that government institutions hold.[252]

Ontario is distinct in that it has both a provincial and municipal version of this statute: the *Freedom of Information and Protection of Privacy Act* (*FIPPA*) and the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*).

Both statutes are largely identical, although *FIPPA* includes some provisions that *MFIPPA* does not. Both aim to provide a right of access to information under the control of institutions, in accordance with stipulated principles:

---

250. *Hopkins v. Kay*, 2015 ONCA 112, 380 D.L.R. (4th) 506, 124 O.R. (3d) 481 (Ont. C.A.) at para. 71, leave to appeal refused *Peterborough Regional Health Centre v. Hesse*, 2015 CarswellOnt 16503, 2015 CarswellOnt 16504, [2015] S.C.C.A. No. 157 (S.C.C.).

251. *Freedom of Information and Protection of Privacy Act*, RSO 1990, c F31 and *Municipal Freedom of Information and Protection of Privacy Act*, RSO 1990, c M56 in Ontario; *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165 in British Columbia; *Freedom of Information and Protection of Privacy Act*, RSA 2000, c F-25 in Alberta; *Freedom of Information and Protection of Privacy Act*, SS 1990-91, c L-27.1 in Saskatchewan; *Freedom of Information and Protection of Privacy Act*, CCSM c F175 in Manitoba; *Right to Information and Protection of Privacy Act*, SNB 2009, c R-10.6 in New Brunswick; *Freedom of Information and Protection of Privacy Act*, SNL 2002, c. A-1.1 in Newfoundland and Labrador; *Access to Information and Protection of Privacy Act*, SNWT 1994, c 20 in Northwest Territories; *Access to Information and Protection of Privacy Act*, SY 1995, c. 1 in the Yukon Territories; *Freedom of Information and Protection of Privacy Act*, RSPEI 1988, c F-15.01 in Prince Edward Island.

252. See for example: *FIPPA*, s 1; *MFIPPA*, s 1.

. information should be public;
. necessary exemptions from the right of access should be limited and specific; and
. decisions on the disclosure of information should be reviewed independently of the institution controlling the information.

Both statutes seek to protect individual privacy with respect to personal information held by institutions, and to grant individuals a right of access to that information.[253] An "institution" under *FIPPA* is either the Assembly, a ministry of the Government of Ontario, a service provider organization under s. 17.1 of the *Ministry of Government Services Act*, a hospital, or an agency, board, commission, corporation, or other body designated as an institution in the regulations.[254]

Under *MFIPPA*, an institution is a municipality, or a municipal-based entity, such as a school board, municipal services board, transit commission, board of health, or planning board.[255]

Both statutes are predominantly focused on accessing records,[256] with specific provisions outlining that the head of the subject institution shall not disclose an individual's personal information to any other person, except where narrow exceptions have been met.[257]

Part III of *FIPPA* and Part II of *MFIPPA* also deal with rules around the collection and retention of individuals' personal information. *FIPPA* has specific requirements for the security and retention of personal information. When personal information collected under Part III of *FIPPA* (dealing with different ministerial data integration units) is stolen, lost, or used or disclosed contrary to the Act, the minister of the subject ministry must notify the individual to whom the personal information relates at the first reasonable opportunity. The individual must be informed that they may make a complaint to the Commissioner.[258]

Both statutes also outline several offences. These include willfully disclosing personal information in contravention of the Act, or willfully maintaining personal information banks that contravene the Act.[259]

---

253. *FIPPA*, s 1; *MFIPPA*, s 1.
254. *FIPPA*, s 2.
255. *MFIPPA*, s 2.
256. *FIPPA*, Part II; *MFIPPA*, Part I.
257. *FIPPA*, s 21; *MFIPPA*, s 14.
258. *FIPPA*, s 49.11.
259. *FIPPA*, s 61; *MFIPPA*, s 48.

However, neither statute requires that a data breach be reported to the Commissioner directly. Nor do they mention a right to a civil claim for breaches of the Acts. This may be because both statutes dictate that heads, or a person acting on behalf or under the direction of a head, are protected from damages resulting from the disclosure or non-disclosure in good faith of a record under the Act, or from a failure to give required notice under the Act.[260]

However, both Acts also make it clear that an institution is not relieved from liability for a tort committed by a head or someone else under each Act.[261]

Labour and Employment

Only British Columbia and Alberta have privacy laws that specifically deal with employee information.[262]

Ontario may join their ranks. On February 28, 2022, Ontario issued Bill 88, the *Working for Workers Act, 2022*,[263] workplace monitoring legislation which will require Ontario employers to give employees notice of "electronic monitoring". These are first-of-their-kind provisions, amendments to the Ontario *Employee Standards Act* entitled "Written Policy on Electronic Monitoring".

All employers with 25 or more employees will be required to create and publish an electronic monitoring policy within 6 months of Bill 88's Royal Assent.[264] The policy must identify whether an employer electronically monitors employees and, if so, must provide (a) a description of how and in what circumstances the employer may electronically monitor employees; and (b) the purposes for which information obtained through "electronic monitoring" may be used by the employer.[265]

Employers must also provide copies of the policy to new and current employees, including employees assigned by temporary help agencies. Interestingly, Bill 88 does not define "*electronic monitoring*". However, it is reasonable to expect that this would include monitoring via corporate networks, personal devices under

---

260. FIPPA, s 62(2); *MFIPPA*, s 49(2).

261. FIPPA, s 62(3); *MFIPPA*, s 49(3).

262. For British Columbia, *Personal Information Protection Act*, SBC 2002, c. 63 and *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165; for Alberta, Alta *PIPA* and *Freedom of Information and Protection of Privacy Act*, RSA 2000, c. F-25.

263. Ontario, Bill 88, *Working for Workers Act, 2022*, 2nd Sess, 42nd Parl, 2002.

264. Ibid., Schedule 2.

265. Ibid., s 41.1.1(2).

"bring your own device" policies, remote networks, and tools with embedded sensors.

It will be interesting to see how Bill 88 will affect employers and what claims employees may bring for violations of the legislation.[266]

Credit Unions and Credit Reporting Agencies

There are provincial laws governing credit unions and the confidentiality of information relating to their members' transactions.[267] There are similar laws for consumer reporting agencies.[268] This is to be expected, given the large volumes of sensitive personal information that these entities collect, affecting individuals' finances and creditworthiness.

In Ontario, the *Consumer Reporting Act* requires consumer reporting agencies to register with the Registrar of Consumer Reporting Agencies. The *Act* obliges the agencies to adopt reasonable procedures for ensuring accuracy and fairness in their reports. It also prohibits access to information, with specific exceptions, and regulates the disclosure of data and contents of consumer reports.

These statutes do not address cybersecurity protections or remedies for breaches expressly. However, their provisions can factor into claims against these sector-specific entities, as standards to be met.

---

266. Bill 88 has been widely regarded as having significant limitations. See the *Comments on Bill 88,* March 24, 2022, of the Information and Privacy Commissioner of Ontario: https://www.ipc.on.ca/wp-content/uploads/2022/03/2022-03-14-ltr-standing-committee-on-social-policy-re-schedule-2-of-bill-88-the-working-for-workers-act-2022.pdf, accessed November 24, 2022.

267. *Credit Unions and Caisses Populaires Act, 1994* SO 1994, c. 11; *Savings and Credit Unions Act*, C-4, 1988, c. 64; *Financial Institutions Act*, RSBC 1996, c. 141; *Credit Union Act*, RSA 2000, c. C-32; *The Credit Union Act, 1998*, SS 1998 c. C-45; *The Credit Unions and Caisses Populaires Act*, CCSM c. C301; *Credit Union Act*, SNS 1994, c-4; *Credit Unions Act*, SNB 1992, c. C-32.3; *Credit Union Act, 2009*, SNL 2009 c. C-37.2; *Credit Unions Act* RSPEI 1988, c. C-29.1; *Credit Union Act* RSNWT (Nu) 1988, c. C-23.

268. *Consumer Reporting Act*, R.S.O. 1990, c. C.33; *Business Practices and Consumer Protection Act*, S.B.C. 2004, c.2; *Personal Investigations Act*, C.C.S.M. c. P34; *Consumer Reporting Act*, R.S.N.S. 1989, with the Registrar of Consumer Reporting Ag c. 93; *Consumer Reporting Act*, R.S.P.E. 1988, c. C-20; *Credit Reporting Act*, S.S. 2004, c. C-43.2; *Consumer Protection and Business Practices Act*, S.N.L. 2009, c. C-31.1.

Part 1 Conclusion: The Statutory Framework and the Future

Cyber threats are evolving continuously. New attack vectors crop up regularly, created to harm Canadians and destroy organizations' cybersecurity.

Canada's statutes have not yet caught up to the cyber threats. Robust cybersecurity legislation may be on the horizon with the introduction of Bill C-26 and the CCSPA, but the mischief remains as evasive as ever.

In the absence of a unitary statutory framework in Canada, one finds several frameworks, a mosaic of protean statutes and regulatory directives which address or seek to address organizational cybersecurity obligations, and individual cybersecurity rights and protections. Determining which framework applies to which organization, or to which individual or group of individuals, is no simple task.

Those seeking to avail themselves of a given framework above must first determine, at a minimum, the nature of the affected information and the type of organization implicated in the cyberattack or cyberbreach.

As new threats or issues arise, courts continue and will likely continue to interpret the statutory frameworks to allow for greater access to the protections under those frameworks.

Expectations continue to shift regarding the cybersecurity risks for which organizations are expected to remain vigilant. Guidance is available. The Privacy Commissioner of Canada has published directives or investigation details regarding some of these risks, including malware, ransomware, spyware, phishing, other forms of spam, and credential stuffing.[269]

There are also sector-specific guidelines, such as the OSFI's guidelines for FRFIs, or IIROC's guidelines for dealer members. While not mandatory, they provide helpful guidance on how institutions both inside and outside the regulators' purview should tackle cybersecurity risks.

As governments and regulators make more refined information readily available, and as organizations become more familiar with

269. Ontario, Office of the Privacy Commissioner of Canada, "Spam" (2020 March 6), online: https://www.priv.gc.ca/en/privacy-topics/technology/ online-privacy-tracking-cookies/online-privacy/spam/, accessed November 24, 2022; Ontario, Office of the Privacy Commissioner of Canada, "Commissioner launches investigation into cyberattacks on Canada Revenue Agency and other federal organizations" (2020 October 13), online: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/an_201013/, accessed November 24, 2022.

cybersecurity risks, the legislative and regulatory standard for precautions to avoid breaches will likely rise. However, whether individual claimants have or will have a statutory cause of action or entitlement to damages for an organization's breach of a specific cybersecurity standard remains unclear.

At present, organizations or institutions are not required to carry out cybersecurity or cyberbreach impact assessments under most of the statutes discussed above. Québec's Bill 64 will require impact assessments when transferring data outside the province. This may establish a widespread standard for cybersecurity safeguards. Organization-specific impact assessment templates may emerge in the near future.

Under *PIPEDA*, damages awards have been largely limited to modest fines or amounts. This reflects the smaller-scale nature of cyberattacks and cyberbreaches involving individuals in past years. As claims for large-scale cyberbreaches become more common, we can expect fines and damage awards to increase commensurately.

Further, if Bill C-26 becomes law or if *CASL* becomes more cyberbreach-focused, we may see greater penalties than those imposed to date. New private law penalties may come into play if *CASL*'s private right of action that would allow individuals to sue violators for damages, comes into force.[270]

The cybersecurity concerns that federal and provincial statutes – including sector-specific legislation – currently address are fairly uniform, but the remedies are not. For example, *PIPEDA* and Alberta *PIPA* offer damages, whereas *FIPPA* and *MFIPPA* are access focused. The federal *Privacy Act* includes no civil remedy for any violation. The *Criminal Code* has penal consequences for cyberbreaches falling under its purview.

The upshot is this: claimants will need to identify their remedial objective when relying on statutes to sue for cyberbreaches.

It will be prudent for practitioners in this area to keep an eye on Bill C-26 and the *CCSPA*. The *CCSPA* is poised to be the first robust cybersecurity legislation in Canada with real consequences for bad actors. It remains to be seen how helpful it will be to individual victims of cyberattacks. Its limited scope may reduce its usefulness for victims of a cybersecurity incident.

The same is true of Bill 64. Regardless of whether an organization operates in Québec, it is important to keep an eye on developments there regarding data governance and management. Cybersecurity

270. The Canadian government suspended the coming into force in 2017, and has not lifted that suspension as of this writing: https://canadagazette.gc.ca/rp-pr/p2/2017/2017-06-14/html/si-tr31-eng.html, accessed November 24, 2022.

and cyberattacks affect all Canadians from coast-to-coast. The policy of one province will often influence what others choose to do.

The legislative dimension of cybersecurity is still developing, especially the remedial rights of individuals. Those statutory rights will likely evolve in conjunction with common law tort remedies.

It is to those common law remedies, as well as liability avoidance strategies, that we will turn in Part 2 of this paper.