International
Comparative
Legal Guides

Practical cross-border insights into cybersecurity

Cybersecurity 2023

Sixth Edition

Contributing Editor:
Edward R. McNicholas
Ropes & Gray LLP

ICLG.com

Expert Analysis Chapters

Q&A Chapters

Canada


Theo Ling


Conrad Flaczyk


Ahmed Shafey


John Pirie

Baker McKenzie

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

Yes, it is an offence to fraudulently obtain, use, control, access or intercept computer systems or functions under the *Criminal Code* (R.S.C., 1985, c. C-46). The relevant provisions of the *Criminal Code* that prohibit hacking (i.e., unauthorised access) are as follows:

- Section 184: Any person who knowingly intercepts a private communication, by means of any electro-magnetic, acoustic, mechanical or other device, is guilty of an indictable offence carrying a maximum penalty of five years' imprisonment.
- Section 342.1: Any person who fraudulently obtains any computer services or intercepts any function of a computer system – directly or indirectly – or uses a computer system or computer password with the intent to do either of the foregoing, is guilty of an indictable offence carrying a maximum penalty of 10 years' imprisonment.
- Recently, in *R. v. Senior*, 2021 ONSC 2729, the Ontario Superior Court summarised the essential elements required for the accused to be found guilty of an offence under Section 342.1 of the *Criminal Code* and found the defendant guilty of unauthorised use of a computer after running a licence plate number contrary to York Regional Police directives.
- Section 380(1): Any person who defrauds another person of any property, money, valuable security or any service is guilty of: (i) an indictable offence carrying a maximum penalty of 14 years' imprisonment where the value of the subject matter of the offence exceeds $5,000; and (ii) an indictable offence or an offence punishable by summary conviction carrying a maximum penalty of two years' imprisonment where the value of the subject matter of the offence is under $5,000.
- Section 430(1.1): Any person who 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, is guilty of: (i) an indictable offence punishable by imprisonment for life if the mischief causes actual danger to life; (ii) an indictable offence or an offence punishable on summary conviction carrying a maximum penalty of 10 years' imprisonment where the value of the subject matter of the offence exceeds $5,000; and (iii) an indictable offence or an offence punishable on summary conviction carrying a maximum penalty of two years' imprisonment where the value of the subject matter of the offence is under $5,000.
- In *R. v. Geller*, [2003] O.J. No. 357, the accused was convicted under Section 430(5) after pleading guilty to "hacking" after obtaining 400 credit card numbers, along with other personal data, and accessing the internet 48 times using false identification.

Denial-of-service attacks

Yes. Under Section 430(1.1) of the *Criminal Code*, it is an offence to obstruct, interrupt or interfere with the lawful use of computer data or to deny access to computer data to a person who is entitled to access it; the maximum penalty for such an offence is 10 years' imprisonment where the offence relates to property with a value exceeding $5,000.

Phishing

Yes. Phishing may constitute fraud under Section 380(1) of the *Criminal Code*. For example, in *R. v. Usifoh*, 2017 ONCJ 451, the accused was convicted of fraud relating to an email phishing scam emanating out of Nigeria and Dubai where he lured victims into sending funds. The maximum penalty for offences under Section 380(1) of the *Criminal Code* is 14 years' imprisonment.

In addition, while not a criminal offence, *Canada's anti-spam legislation* ("*CASL*"), prohibits the sending of unsolicited commercial electronic messages ("CEMs"). Under section 20(4) of *CASL*, any person who contravenes *CASL* may be subject to a maximum administrative monetary penalty of up to $1 million in the case of an individual, and up to $10 million in the case of any other person.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Yes. Under Section 430(1.1) of the *Criminal Code*, it is an offence to commit mischief in connection with computer data, as noted above. The maximum penalty for such an offence is 10 years' imprisonment where the value of property in question exceeds $5,000; however, if a human life is endangered, offenders can be liable to life imprisonment.

In addition, Section 8(1) of *CASL* prohibits anyone in the course of a commercial activity, regardless of an expectation of profit, to: (i) install or cause to be installed a computer program on any other person's computer system; or (ii) cause an electronic message to be sent from that computer system, unless

they receive the express consent of the computer system's owner or an authorised user, or if the person is acting in accordance with a court order.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime

Yes. It is an offence under Section 342.2 of the *Criminal Code* to – without lawful excuse – sell or offer for sale a device that is designed or adapted primarily to commit cybercrime, knowing that the device has been used or is intended to be used to commit a cybercrime that is prohibited under Sections 342.1 or 430 of the *Criminal Code* (described in more detail above).

The definition of "device" in Section 342.2 of the *Criminal Code* includes: (i) the component of a device; and (ii) a computer program (i.e., computer data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function).

The maximum penalty under Section 342.2 is two years' imprisonment. If a person is convicted of an offence, forfeiture of any device relating to the offence may also be ordered.

Possession or use of hardware, software or other tools used to commit cybercrime

Yes. It is an offence under Section 342.2 of the *Criminal Code* to – without lawful excuse – possess, import, obtain for use, distribute, or make available a device that is designed or adapted primarily to commit cybercrime, knowing that the device has been used or is intended to be used to commit a cybercrime that is prohibited under Sections 342.1 or 430 of the *Criminal Code* (described in more detail above).

The maximum penalty is the same as noted above – i.e., two years' imprisonment and, if a person is convicted of an offence, forfeiture of any device relating to the offence may also be ordered.

Identity theft or identity fraud (e.g. in connection with access devices)

Yes. Sections 402.2 and 403 of the *Criminal Code* prohibit identity theft and identity fraud, respectively.

With respect to identity theft, it is an offence to obtain or possess another person's identity information with the intent to use it to commit an indictable offence like fraud, deceit, or falsehood. Furthermore, any person who transmits, makes available, distributes, sells or offers another person's identity information for the same purposes will be guilty of a criminal offence

Regarding identity fraud, it is an offence to fraudulently personate another person, living or dead, with the intent to: (i) gain advantage for themselves or another person; (ii) obtain any property or interest in any property; (iii) cause disadvantage to the person being personated or another person; or (iv) avoid arrest or prosecution or to obstruct, pervert or defeat the course of justice.

Notably, the *Criminal Code* does not limit the aforementioned offences to any medium – e.g., online, through access devices, or otherwise.

The maximum penalty for identity theft under Section 402.2 is five years' imprisonment, and the maximum penalty for identity fraud under Section 403 is 10 years' imprisonment.

In *R. v. Mackie*, 2014 ABCA 221, the accused pled guilty to 39 criminal charges, including three counts of identity fraud (and unauthorised use of a computer), after accessing the Facebook accounts of minors and personating those minors' friends to lure them into making child pornography.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Electronic theft is not specifically covered by the *Criminal Code*; however, depending on how the electronic theft is carried out and what is stolen, it may be considered an indictable offence under one of the many prohibitions against fraudulent transactions found in the *Criminal Code*. For example, any deceit, falsehood, or fraud by a current or former employee in order to knowingly obtain a trade secret, or communicate or make available a trade secret, is prohibited under Section 391(1) of the *Criminal Code*. Similarly, it is an offence under Section 342.1 of the *Criminal Code* to fraudulently obtain any computer service, which includes data processing and the storage or retrieval of computer data.

In addition to the foregoing, Section 322 of the *Criminal Code* deals with theft generally. Many of the prohibitions in Section 322 against theft would cover electronic theft as well. For example, a person commits theft when he/she fraudulently and without colour of right takes or converts to his/her use anything with intent to deprive – temporarily or absolutely – the owner of his/her thing, property or interest therein. That said, the Supreme Court of Canada's historical approach to electronic theft is that non-tangible property, other than identity theft, is not considered property (see *R. v. Stewart*, [1988] 1 SCR 963) for the purposes of Section 322 of the *Criminal Code*. This interpretation has since been applied to data and images, which also cannot be the subject of theft under Section 322, although they can be the subject of other criminal offences (see, e.g., *R. v. Maurer*, 2014 SKPC 118; *ORBCOMM Inc. v. Randy Taylor Professional Corp.*, 2017 ONSC 2308).

It is also a criminal offence to circumvent technological protection measures, or manufacture, import, distribute, offer for sale or rental, or provide technology, devices, or components for the purposes of circumventing technological protection measures under Section 41.1 of the *Copyright Act*. Knowingly circumventing technological protection measures for commercial purposes is a criminal offence under Section 42(3.1) of the *Copyright Act*, and can carry a maximum penalty of a $1 million fine and/or five years' imprisonment.

Canadian privacy laws, including legislation relating to personal health information, also contain provisions prohibiting the unauthorised collection, use, disclosure and access to personal information ("PI"). For example, under Section 107 of Alberta's *Health Information Act*, RSA 2000, c. H-5, it is an offence to collect, gain, or attempt to gain access to personal health information in contravention of the Act (e.g., by way of electronic theft without the authorisation of the relevant data subject); the maximum penalty for such an offence is a fine of $200,000 for individuals, and $1 million for any other person.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)

Yes. Unsolicited penetration testing may be considered an offence under Section 342.1 of the *Criminal Code*. Under Section 342.1, individuals are prohibited from fraudulently, and without colour of right, obtaining, directly or indirectly, any computer service, or intercepting or causing to be intercepted, directly or indirectly, any function of a computer system. Unsolicited penetration testing may also be considered mischief under Section 430(1.1) of the *Criminal Code*, as detailed above.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Yes. Pursuant to Section 184 of the *Criminal Code*, it is an offence for any person to knowingly intercept a private communication by means of any electro-magnetic, acoustic, mechanical, or other device, which is punishable by a maximum penalty of five years' imprisonment. Although the concept of "intercepting"

generally requires the listening or recording of contemporaneous communication, in *R. v. TELUS Communications Co.*, [2013] 2 SCR 3, unlawful interception also applied to the seizing of text messages that were stored on a telecommunication provider's computer.

Moreover, under Section 83.2 of the *Criminal Code*, any person who commits an indictable offence under this or any other Act of Parliament for the benefit of, at the direction of or in association with a terrorist group is guilty of an indictable offence and liable to imprisonment for life. The definition of a "terrorist activity" under Section 83.01 includes an act that causes serious interference with 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 may include "cyberterrorism".

Under Section 19 of the *Security of Information Act* (R.S.C., 1985, c. O-5), it is also 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. The maximum penalty under Section 19 is 10 years' imprisonment.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Section 6(2) of the *Criminal Code* states that "no person shall be convicted … of an offence committed outside Canada". That said, Canadian courts will exercise jurisdiction over an offence where there is a "real and substantial" link between that offence and Canada; a "real and substantial link" may exist where a significant portion of the activities constituting the offence occurred in Canada (see *R. v. Libman*, [1985] 2 SCR 178). Because cybercrime takes place online, the location of the server or computer is not always indicative of the location of the crime; therefore, the aforementioned offences may have extraterritorial application depending on the specific circumstances surrounding the relevant offence (i.e., whether there is a "real and substantial link" to Canada).

Moreover, Section 26(1) of the *Security of Information Act* considers any person who commits an offence outside Canada to have committed the offence in Canada if the person is: (i) a Canadian citizen; (ii) a person who owes allegiance to Her Majesty in right of Canada; (iii) a person who is locally engaged and who performs his/her functions in a Canadian mission outside Canada; or (iv) a person who, after the time the offence is alleged to have been committed, is present in Canada.

Violations under *CASL* similarly have the potential for extraterritorial application. Section 12 of *CASL* applies to all CEMs accessed in Canada, including those sent from another country, and Section 8 prohibits the installation of computer programs without the express consent of the owner or authorised user of a computer system in Canada; this prohibition applies so long as the computer system is located in Canada.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

For criminal offences in Canada, there are no specific factors that would mitigate a penalty. Sentencing for criminal offences is assessed case by case, and Sections 718–718.21 of the *Criminal Code* provide guiding principles therefor. Some of the more relevant sentencing guidelines set out in the *Criminal Code* are outlined below.

- Section 718.1: "A sentence must be proportionate to the gravity of the offence and the degree of responsibility of the offender."
- Section 718.2(a): "A sentence should be increased or reduced to account for any relevant aggravating or mitigating circumstances relating to the offence or the offender."
- Section 718.21: This Section sets out a list of "additional factors" that courts will consider when imposing a sentence, including the "degree of planning involved in carrying out the offence and the duration and complexity of the offence".

There are also exceptions established under the *Copyright Act* that allow for circumvention of technological protection measures under certain circumstances. For example, Section 42(3.1) carves out any person acting on behalf of a library, archive or museum or educational institution from criminal liability for circumventing technological protection measures. Similarly, under Section 41.11, circumvention of technological protection measures is allowed for the purposes of national security.

Section 6 of *CASL* also provides for exceptions to the prohibition on unsolicited CEMs, including but not limited to messages that are sent by or on behalf of an individual to another individual with whom they have a personal or family relationship, or if the recipient of the communication has given express consent.

2 Cybersecurity Laws

2.1 *Applicable Laws*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

The *Criminal Code* prohibits the unauthorised use of a computer (Section 342.1), the possession of a device to obtain unauthorised use of computer system or to commit mischief (Section 342.2), and mischief in relation to computer data (Section 430(1.1)).

Section 19 of the *Security of Information Act* and Section 391(1) of the *Criminal Code* also prohibit fraudulently obtaining or communicating a trade secret.

CASL protects consumers and businesses from the misuse of digital technology, including spam and other electronic threats, by prohibiting – in the course of commercial activity – (i) the alteration of transmission data in an electronic message so that the message is delivered to a destination other than or in addition to that specified by the sender (Section 7(1)), (ii) the installation of a computer program on any other person's computer system without express consent or court order (Section 8(1)), and (iii) the sending of a CEM to an electronic address in order to induce or aid any of the above (Section 9).

Sections 41 and 42 of the *Copyright Act* provide for civil and criminal remedies related to technological protection measures and rights management information.

There are various privacy statutes in Canada that regulate the way in which PI can be collected, used or disclosed:

- Canada's federal privacy legislation – the *Personal Information Protection and Electronic Documents Act* ("*PIPEDA*") – applies to private-sector organisations across Canada that collect, use or disclose PI in the course of commercial activity. Federally regulated organisations that conduct business in Canada are also subject to the *PIPEDA*, including their collection, use or disclosure of their employees' PI.

- Canada's federal government has proposed amendments in *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* ("*Digital Charter Implementation Act, 2022*"), which, if it were to pass, would enact the *Consumer Privacy Protection Act*, effectively replacing provisions under the *PIPEDA* applying to the collection, use, and disclosure of PI in the course of commercial activities, including breach reporting and notification provisions, security safeguard provisions, and a right of action would be created for violations of the *Consumer Privacy Protection Act*.
- Alberta, British Columbia and Québec have their own private-sector privacy laws that have been deemed substantially similar to the *PIPEDA*. Organisations subject to a substantially similar provincial privacy law are generally exempt from the *PIPEDA* with respect to the collection, use or disclosure of PI that occurs within that province; however, the *PIPEDA* may apply where PI collected in Alberta, British Columbia, or Québec is moved across provincial or national boundaries or with respect to the collection, use, and disclosure of personal information from federally regulated employees in Canada. Depending on the circumstances, provincial privacy laws may apply in conjunction with the *PIPEDA*.
- On September 22, 2021, Québec passed Bill 64, *An Act to modernise legislative provisions as regards the protection of personal information* ("Bill 64"), which will gradually enter into force from September 22, 2022, with the majority of provisions entering into force on September 22, 2023. The remaining provisions will enter into force on September 22, 2024. Bill 64 will bring significant amendments to Québec's private sector privacy law, *An Act respecting the protection of personal information in the private sector* ("*QC Privacy Law*"), such as the introduction of prescribed breach reporting and notification obligations, requirements to conduct a privacy impact assessment where PI is communicated outside of Québec or where information systems are created or overhauled, and express consent requirements where "sensitive" PI is collected.
- New Brunswick, Newfoundland and Labrador, Nova Scotia and Ontario have also adopted substantially similar legislation regarding the collection, use and disclosure of personal health information.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

Many departments and agencies across the Canadian government play a role with respect to cybersecurity in Canada for critical infrastructure and operators of essential services. All of these organisations engage with Public Safety Canada ("PS"); PS is the department responsible for ensuring coordination across all federal departments and agencies responsible for national security and the safety of Canadians and has released guidance on the fundamentals of cybersecurity for Canada's critical infrastructure community.

Working with PS, the Communication Securities Establishment ("CSE") is the technical authority in Canada for cybersecurity and information assurance. The *Communications Security Establishment Act* (S.C. 2019, c. 13) ("*CSEA*") mandates the CSE to acquire, use and analyse information from the global information infrastructure, or from other sources, to provide advice, guidance and services to protect electronic information and information infrastructures. The CSE guides IT security specialists in the federal government through various IT security directives, practices and standards.

As part of its mandate, the CSE operates the Canadian Centre for Cyber Security and issues alerts and advisories on potential, imminent or actual cyber threats, vulnerabilities or incidents affecting Canada's critical infrastructure, which includes alerts on cyber threats to Canadian health organisations.

On June 14, 2022, the Government of Canada introduced Bill C-26, which, if passed, would amend Canada's *Telecommunications Act* to implement new cybersecurity protections for telecommunications services providers in Canada. Most notably, Bill C-26 would provide the federal government with new regulatory powers to order telecommunications services providers to take certain affirmative actions or to restrict their services or operations where it is deemed "necessary" to mitigate or remedy cybersecurity risks. Such actions and restrictions could include, among others, prohibiting the use of certain suppliers, prohibiting the supply of services to certain customers, or restricting services that pose a significant cybersecurity risk.

If passed, Bill C-26 would also enact the *Critical Cyber Systems Protection Act* ("*CCSPA*"). The *CCSPA* would impose obligations on operators of any "critical cyber system" in Canada, which is defined under Bill C-26 as any cyber system that, if compromised, could affect the continuity or security of a "vital system" or service. Schedule 1 of the *CCSPA* defines a "vital system" as including federally regulated cyber systems, such as those of banks and telecommunications services providers, among others. If passed, operators of critical cyber systems would have an obligation to create a cybersecurity program meeting a number of prescribed safeguards, and an obligation to notify their respective regulators of their programs. These operators would also have new breach reporting obligations *vis-à-vis* their respective regulators where a cybersecurity incident could interfere with the continuity of a vital system or service.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Yes. Organisations have an obligation under privacy laws in Canada to protect PI; an organisation's responsibilities include breach reporting, notification, and recording obligations in the event that an incident impacts PI.

For example, the *PIPEDA* requires organisations to protect PI by implementing security safeguards to protect against loss or theft thereof, as well as unauthorised access, disclosure, copying, use or modification. The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution and format of the information, and the method of storage. The methods of protection may include technological measures like using passwords and encryption. As noted at question 2.1, federal Bill C-27 proposes to enact the *Consumer Privacy Protection Act*, which, if passed, would effectively replace the *PIPEDA* with respect to obligations on safeguarding PI and responding to breaches.

Financial regulators in Canada also require or expect certain organisations to monitor, detect, prevent, or mitigate incidents, as detailed below:

- The Office of the Superintendent of Financial Institutions ("OSFI") issued an updated *Technology and Cyber Security Incident Reporting Advisory* document, which supports a coordinated and integrated approach to the OSFI's awareness

of, and response to, technology and cybersecurity incidents at Federally Regulated Financial Institutions ("FRFIs"). In July 2022, OSFI also issued the final version of guideline B-13, which sets out OSFI's expectations with respect to the use of technology by FRFIs and cyber risk management best practices.

- The Investment Industry Regulatory Organisation of Canada ("IIROC") provides various cybersecurity resources for Dealer Members to follow, including guides to help dealers protect themselves and their clients against cyber threats and attacks. The IIROC has also implemented rules for its Dealer Members to report cybersecurity incidents.
- The Canadian Securities Administrator ("CSA") issues cybersecurity-related staff notices, including: (i) CSA Staff Notice 11-326 (Cyber Security) to inform issuers, registrants and regulated entities on risks of cybercrime and steps to address these risks; (ii) CSA Staff Notice 11-338 (CSA Market Disruption Coordination Plan) to inform market participants about the CSA's coordination process to address a market disruption, including one that may stem from a large-scale cybersecurity incident; (iii) CSA Staff Notice 33-321 (Cyber Security and Social Media) to inform firms on cybersecurity risks associated with social media use; and (iv) CSA Staff Notice 11-332 (Cyber Security). Organisations regulated by the CSA are expected to conduct a cybersecurity risk assessment annually.
- The Mutual Fund Dealers Association of Canada ("MFDA") provides a Cybersecurity Assessment Program that offers mutual fund dealers assessments of their cybersecurity practices and advice on improving their defences. The MFDA released bulletins on cybersecurity to enhance member awareness and understanding of cybersecurity issues and resources and provide guidance regarding the development and implementation of cybersecurity procedures and controls.

In addition to the foregoing, the *Telecommunications Act* mandates telecommunications service providers to protect the privacy of their users through the provision of various consumer safeguards.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Organisations subject to the *PIPEDA* are required to report to the Office of the Privacy Commissioner of Canada ("OPC") any breaches of security safeguards involving PI that pose a real risk of significant harm to individuals. The *PIPEDA* also requires organisations to keep records of any incident involving loss of, unauthorised access to or unauthorised disclosure of PI due to a breach of (or failure to establish) the security safeguards required by the *PIPEDA*, and prescribes the minimum content for reports to the OPC, including but not limited to:

- a description of the incident;
- the timing of the incident;
- the PI impacted;
- an assessment of the risk of harm to individuals as a result of the breach;
- the number of individuals impacted;
- the steps to mitigate and/or reduce the risk of harm; and
- the name and contact information for a person at the organisation who can be contacted about the breach.

Similar breach reporting and notification requirements are found under other data protection statutes, including private-sector legislation in Alberta, public-sector legislation in the Northwest Territories and Nunavut, and legislation applicable to personal health information custodians in Ontario and Alberta. As of September 22, 2022, breach reporting and notification requirements will also enter into force under a regulation to Québec's Bill 64, amending the *QC Privacy Law*.

Financial regulators such as the CSA, OSFI, IIROC, and MFDA also require the reporting of incidents. These incident reporting obligations generally pertain to any material systems issues, cybersecurity or technology risks and incidents, security breaches, breaches of client confidentiality or system intrusion. While it has neither passed nor entered into force, federal Bill C-26 would enact the *Critical Cyber Systems Protection Act*, which would impose breach reporting obligations on operators of a "critical cyber system" where a breach or suspected breach could impact the continuity of a vital system or service. Schedule 1 defines a "vital system" as a system as including federally regulated systems, such as those provided by banks or telecommunications services providers. Operators of critical cyber systems would have breach reporting obligations towards their respective regulators if Bill C-26 were to pass.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

The *PIPEDA* and Alberta's *Personal Information Protection Act* ("*PIPA*") require private-sector organisations to notify data subjects of certain breaches of their PI. However, under Alberta's *PIPA*, in the event of a breach, the regulator, upon reviewing the Breach Report Form submitted by an organisation, will determine and instruct the organisation whether it needs to notify individual data subjects. Moreover, as of September 22, 2022, notification obligations will also enter into force in Québec under a regulation to Bill 64, amending the *QC Privacy Law*. There will generally be a duty to notify data subjects of a data breach that presents a "risk of serious injury" to an individual data subject. Breach notification obligations might also be triggered under provincial privacy laws that apply to public institutions or health information custodians. For example, provincial health privacy laws in New Brunswick, Newfoundland and Labrador and Ontario also have reporting requirements relating to the healthcare industry.

In particular, organisations subject to the *PIPEDA* are required to notify affected individuals about breaches of security safeguards involving PI that pose a real risk of significant harm to those individuals as soon as feasible. The notification must include enough information to allow the individual to understand the significance of the breach to them and to allow them to take steps, if any are possible, to reduce the risk of harm that could result from the breach. Other content and the manner of delivering the notice may be prescribed under the *PIPEDA* as well.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The Canadian Radio-television and Telecommunications Commission ("CRTC"), the OPC and the Competition Bureau are respectively mandated to enforce *CASL*, the *CASL*-related provisions of the *PIPEDA* and the *CASL*-related provisions of the *Competition Act* (R.S.C., 1985, c. C-34).

The OPC oversees compliance with the *PIPEDA*. There are certain offences under the *PIPEDA* that can be prosecuted by the Attorney General. Each provincial regulator is responsible for enforcing their provincial privacy statutes.

The Competition Bureau, an independent law enforcement agency, may also investigate false and misleading statements concerning consumers' privacy as a violation of the *Competition Act*.

See also the financial industry-specific regulators described in question 2.3, which regulate compliance with their industry-specific cybersecurity policies, guidelines and requirements.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

The OPC has the power to investigate complaints, audit and make non-binding recommendations in response to privacy violations. Upon the OPC's decision, an application can be made to the Federal Court for damages to complainants. The Attorney General can prosecute an organisation for failure to comply with the breach reporting, notification and recording obligations under the *PIPEDA*, which can result in fines of up to $10,000 on summary conviction or $100,000 for an indictable offence. Some of the provincial data protection statutes (e.g., in British Columbia and Alberta) also provide for fines of up to $100,000 in the event of non-compliance.

The proposed *Digital Charter Implementation Act, 2022* – or any revised version thereof, if passed – may give the OPC new enforcement powers as well, including the ability to make binding orders and have the power to recommend fines to the new Personal Information and Data Protection Tribunal, established by the *Personal Information and Data Protection Tribunal Act* (not yet passed). This new privacy-focused tribunal would hear appeals from OPC orders and make decisions on whether to issue fines against organisations. Decisions from the Personal Information and Data Protection Tribunal would be final and binding, subject only to judicial review on procedural grounds. Furthermore, the *Consumer Privacy Protection Act* (not yet passed) would allow the tribunal to impose fines of up to 3% of an organisation's gross global revenue or $10 million, whichever is higher. For more egregious offences, the Tribunal can issue fines of up to 5% of an organisation's gross global revenue or $25 million, whichever is higher.

Any organisation that makes false and misleading statements concerning consumers' privacy may also be subject to fines of up to the greater of $10 million and 3% of the organisation's gross global revenues in the preceding financial year.

Penalties for criminal offences and non-compliance with *CASL* are described under question 1.1 (under "Phishing").

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

The CRTC has taken enforcement action under *CASL* for violations of Sections 8 and 9, with fines of $100,000 to $150,000 for the unlawful distribution of advertisements through the offending parties' services.

The OPC regularly investigates incidents involving breaches of PI, including, for example:

- *PIPEDA* Findings #2021-001 – Joint investigation by federal and provincial privacy commissioners (Alberta, British Columbia and Québec) to examine whether Clearview AI, Inc.'s collection, use and disclosure of PI by means of its facial recognition tool complied with federal and provincial privacy laws applicable to the private sector.
- *PIPEDA* Findings #2020-005 – Investigation into Desjardins for a breach of security safeguards that affected close to 9.7 million individuals in Canada and abroad.
- *PIPEDA* Findings #2019-001 – Investigation into Equifax Inc. and Equifax Canada Co.'s compliance with the *PIPEDA* regarding a breach of security safeguards resulting in the disclosure of PI in 2017.
- *PIPEDA* Findings #2021-003 – Security deficiencies at a large financial institution leading to a large-scale breach; improvements to security safeguards were made and matter resolved.
- *PIPEDA* Findings #2022-001 – Joint investigation into Tim Hortons' location tracking in mobile app; investigation found that location data not collected for an appropriate purpose.
- *PIPEDA* Findings #2021-003 – Fido's employees bypassed authentication protocols allowing fraudsters to repeatedly access customer's account.
- *PIPEDA* Findings #2016-005 – Investigation of Ashley Madison in connection with hacking and online posting of users' account information, which lead to OPC recommendations.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems)?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)

Canadian privacy laws require users to provide consent to and/or be provided with sufficient notice of the collection, use and disclosure of their PI, and an opportunity to withdraw such consent.

The OPC's Guidelines for identification and authentication provide that because devices are usually associated with individuals, the metadata collected from devices through tracking mechanisms (i.e., beacons) can be used to identify an individual without their knowledge. The metadata collected from such devices could include PI, the use of which may be considered surveillance or profiling. It is possible that certain exceptions under Canadian privacy laws may apply to the use of beacons (i.e., Section 7(1)-(2) of the *PIPEDA*); the use thereof should be evaluated on a case-by-case basis.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)

The use of honeypots is not expressly prohibited under applicable Canadian laws and, to our knowledge, there is currently no case law that provides further guidance. That said, the general application of Canadian privacy laws relating to the collection, use or disclosure of PI applies notwithstanding that they may

be used defensively. The exceptions above relating to the use of beacons may also apply; however, such exceptions should also be evaluated on a case-by-case basis.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
The use of sinkholes is not expressly prohibited under applicable Canadian laws and, to our knowledge, there is currently no case law that provides further guidance. That said, the general application of Canadian privacy laws relating to the collection, use or disclosure of PI applies notwithstanding that they may be used defensively. The exceptions above relating to the use of beacons and honeypots may also apply; however, such exceptions should also be evaluated on a case-by-case basis.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber attacks?

Employee monitoring is generally permissible under Canada's privacy legislation, but it must be carried out in compliance with such laws, and for a reasonable purpose, such as preventing, detecting, mitigating and responding to cyberattacks.

On April 11, 2022, Ontario's Bill 88, *Working for Workers Act, 2022*, received Royal Assent and amends Ontario's *Employment Standards Act*. By October 11, 2022, Ontario employers with 25 or more employees are obligated to have a written electronic monitoring policy in place in that sets out: (1) whether the employer electronically monitors employees and, if so, a description of how and in what circumstances the employer electronically monitors employees; and (2) the purposes for which information obtained through electronic monitoring may be used by the employer. The electronic monitoring policy must also be shared with employees, and the date that the policy was published and the dates of all updates must be included on the policy.

Privacy regulators use a reasonableness test set out in *Eastmond v. Canadian Pacific Railway*, 2004 FC 852, with regard to the collection of employee PI, which can be used in determining the reasonableness of a monitoring programme:

- Can it be demonstrated that monitoring is necessary to meet a specific need?
- Is the monitoring likely to be effective in meeting that need?
- Is any loss of privacy proportional to the benefit gained?
- Could the employer have met the need in a less privacy-invasive way?

While this has received subsequent negative treatment, the OPC still refers to this case in its findings. For example, *PIPEDA* Report Findings #2021-001, Joint investigation of Clearview AI, cites this case in the context of assessing whether the purpose for collecting PI was appropriate.

Notification must be given for such a monitoring programme; for example, through an employee privacy policy. Monitoring employees in a unionised setting must be in compliance with applicable collective agreements and employee monitoring measures must comply with Canadian labour laws.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber attacks?

Canada has export controls in place to ensure that exports of certain goods and technology (e.g., military and dual-use technologies) are consistent with national foreign and defence policies. The *Export and Import Permits Act* (R.S.C., 1985, c. E-19) authorises the Minister of Foreign Affairs to issue permits to export items included on the Export Control List or to a country included on the Area Control List, subject to certain terms and conditions. Factors impacting the need for a permit include the nature, characteristics, origin or destination of the goods or technology being exported.

The Department of Foreign Affairs, Trade and Development published a Guide to Canada's Export Control List, which addresses the trade of encryption items – i.e., systems, equipment and components designed or modified to use cryptography for data confidentiality – under Category 5, Part 2: "Information Security". Due to its inclusion on the Export Control List, encryption or cryptographic technologies require an export permit such as the General Export Permit No. 45 — Cryptography for the Development or Production of a Product (SOR/2012-160).

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Market practices relating to information security usually do not vary substantially across business sectors. Certain sectors have supplementary information security requirements and/or recommendations (see question 4.2). Many organisations will also commit to a higher standard of information security beyond what is strictly required for compliance with sector-specific statutory requirements. For example, payment processors in Canada will usually choose to comply with the Payment Card Industry Data Security Standard ("PCI DSS"), a set of security standards overseen by an independent body, designed to ensure that organisations that accept, process, store or transmit credit card information maintain a secure environment.

The public sector also has specific information security requirements for all levels of government. For example, the *Privacy Act* (R.S.C. 1985, c. P-21) governs the PI-handling practices of federal government institutions and applies to all of the PI that the federal government collects, uses and discloses. Canadian provinces, territories and municipalities have enacted similar legislation regulating the PI-handling practices of government institutions under their respective jurisdictions.

4.2 Excluding the requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Yes, there are industry-specific requirements relating to cybersecurity in Canada.

Financial services providers must comply with federal and provincial laws that include specific provisions dealing with the protection of PI. For example, the Canadian *Bank Act* (S.C. 1991, c. 46) contains provisions regulating the use and disclosure of personal financial information and, through the enactment of regulations, may mandate Canadian banks to establish procedures for restricting the collection, retention, use and disclosure of personal financial information. Provincial laws governing

credit unions also typically contain provisions dealing with the confidentiality of information relating to members' transactions. In addition, many provinces have laws that deal with consumer credit reporting, and these typically impose obligations on credit reporting agencies to ensure the accuracy and limit the disclosure of information. Financial service regulators have also published various recommendations relating to cybersecurity, including a series of guidelines developed by the Bank of Canada, Department of Finance and OSFI in collaboration with other G-7 partners.

Telecommunications service providers are also obligated to protect the privacy of their users by providing various consumer safeguards under the *Telecommunications Act*. The Canadian Security Telecommunications Advisory Committee ("CSTAC"), established to support Canada's National Strategy for Critical Infrastructure and Canada's Cyber Security Strategy, has published several guidance and best practice documents that telecommunications service providers should follow, including: (i) Security Best Practice Policy for CTSPs; (ii) Critical Infrastructure Protection Standard for CTSPs; (iii) Network Security Monitoring and Detection Standard for CTSPs; (iv) Security Incident Response Standard for CTSPs; and (v) Information Sharing, Reporting and Privacy Standard for CTSPs. As noted in question 2.1, federal Bill C-26 proposes to amend the *Telecommunications Act* to provide the federal government with powers to impose restrictions and order telecommunications service providers to take certain actions to mitigate and remedy cybersecurity risks impacting their services, operations, and customers.

Organisations in both the financial and telecommunication sectors must comply with the *PIPEDA*, including in relation to requirements regarding the PI of employees since business in both sectors is classified as a "federal work, undertaking or business".

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

Under Canadian law, directors owe a fiduciary duty to their company to act in its best interests, and to exercise the care, diligence and skill that a reasonably prudent person would exercise in comparable circumstances, and can be liable for failing to satisfy such duty. These duties include an obligation to act prudently in the company's interests with regard to cybersecurity. Failure to take appropriate action to remedy known cybersecurity concerns that a reasonable person would have remedied could expose directors to personal liability. Directors and officers may also be exposed to personal liability for failures to adequately and truthfully represent an organisation's cybersecurity measures, or for failures to disclose cybersecurity incidents and risks.

In the event of a breach of duties, a due diligence defence may apply, where the director or office acted in good faith and at the guidance of professionals. For example, Section 54 of *CASL* sets out the due diligence defence for certain Sections of *CASL*, the *PIPEDA*, and the *Competition Act*.

Directors or officers may also be found personally liable under provincial privacy legislation as seen, by way of example, in Section 93 of the *QC Privacy Law* respecting the protection of PI in the private sector, C.Q.L.R c. P-39, and Section 64(2) of Manitoba's *Personal Health Information Act*, C.C.S.M. c. P33.5. In Québec, Bill 64 will amend the *QC Privacy Law* to increase director liability up to $100,000 if they knowingly fail to report a breach.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Under Canadian privacy laws (e.g.: Schedule 1, Principle 4.1 of the *PIPEDA*; Section 5 of Alberta's *PIPA*; and Section 4 of BC's *PIPA*), organisations are required to appoint an individual, or individuals, responsible for compliance with obligations under the respective statutes, including compliance with requirements relating to security safeguards. As Canadian privacy laws do not specify a particular title, these individuals may, for example, be referred to as the "Privacy Officer" or "Chief Information Security Officer". In Québec, Bill 64 will amend the *QC Privacy Law* to require that a person within an enterprise "exercising the highest authority" shall ensure that the Act is implemented and complied with in all material respects.

Canadian privacy regulators have issued guidance documents, published findings and provided best practice recommendations for organisations to have established incident response plans and policies in place, conduct cyber risk assessments, and perform penetration tests/vulnerability assessments. While there is no strict requirement to abide by these guidance documents, failing to do so may result in non-compliance with an organisation's obligations under applicable privacy laws.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Section 45 of Québec's *Act to Establish a Legal Framework for Information Technology*, c. C-1.1, requires the disclosure of any creation of a database of biometric characteristics and measurements to the Commission d'accès à l'information. Bill 64 will amend the *QC Privacy Law* to require that businesses disclose their database of biometric characteristics to the Commission d'accès à l'information "no later than 60 days before it is brought into service".

Other laws within Canada may contain additional disclosure requirements, and organisations should confirm this on a case-by-case basis.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

An individual can enforce their rights by making a complaint to any of the privacy regulatory authorities mentioned in question 2.6 (or any other regulator discussed in this chapter). A complaint may be made relating to an organisation's failure to comply with any of its statutory obligations to collect, use and disclose PI in accordance with the principles of fair information practices set out in Canada's privacy legislation:

- accountability;
- identifying purpose;
- consent;
- limiting collection;
- limiting use, disclosure and retention;
- accuracy;
- safeguards;

- openness;
- individual access; and
- challenging compliance.

These authorities are generally required to investigate any such complaint.

Under the *PIPEDA*, a formal complaint must be investigated, and the OPC will issue a report outlining the findings of the investigation and any recommendations for compliance. The report may be made public at the discretion of the OPC. While it has neither passed nor entered into force, federal Bill C-27 proposes to enact the *Personal Information and Data Protection Tribunal Act*, which would establish an administrative tribunal to hear appeals of decisions made by the Privacy Commissioner of Canada under the proposed *Consumer Privacy Protection Act*. Decisions made by the administrative tribunal would be final and binding, subject only to judicial review on procedural grounds.

The *Consumer Privacy Protection Act* would create a new private right of action for individuals affected by an act or omission that constitutes a contravention of the *Consumer Privacy Protection Act*. The cause of action would allow individuals to pursue organisations for violations and claim damages for loss or injury suffered as a result of contraventions of the Act. The private right of action would extend to a number of offences, ranging from the failure of an organisation to implement and maintain a privacy management program to failures to dispose of PI upon the request of individuals.

Under Alberta's *PIPA* and BC's *PIPA*, an investigation may be elevated to a formal inquiry by the Commissioner and result in an order. Organisations are required to comply with the order, or apply for judicial review, within a prescribed time period. Similarly, under the *QC Privacy Law*, an order must be obeyed within a prescribed time period. An individual may appeal to a judge of the Court of Québec on questions of law or jurisdiction with respect to a final decision.

Additionally, class action lawsuits are common in the aftermath of an incident that results in the breach of PI. The most common causes of action advanced in class actions are:

- breach of confidence;
- breach of contract;
- breach of fiduciary duty;
- breach of Section 7 of the Canadian Charter of Rights and Freedoms;
- breach of the *PIPEDA* or the *Privacy Act*;
- breach of provincial privacy legislation;
- invasion of privacy:
- intrusion on seclusion; and
- publicity to private life (public disclosure of embarrassing private facts);
- negligence; and
- unjust enrichment.

The invasion of privacy torts is relatively new in the Canadian legal landscape. The tort of intrusion on seclusion was recognised in the Ontario Court of Appeal case *Jones v. Tsige*, 2012 ONCA 32. While this case has received subsequent negative treatment, the private right of action "tort of intrusion on seclusion" outlined in this case continues to be considered in subsequent cases: *Broutzas v. Rouge Valley Health System*, 2018 ONSC 6315. The tort of public disclosure of embarrassing private facts was recognised by the Ontario Superior Court in *Jane Doe 464533 v. ND (Jane Doe)*, 2016 ONSC 541.

The legal test for the tort of intrusion on seclusion requires objective proof that the alleged invasion of privacy would be highly offensive to a reasonable person.

The legal test for the tort of public disclosure of private facts requires proof that the matter publicised (the private facts) or was an act of publication: (a) would be highly offensive to a reasonable person; and (b) is not of legitimate concern to the public.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

In *Chitrakar v. Bell TV*, 2013 FC 1103, the Federal Court awarded the plaintiff over $20,000 in damages following a privacy violation by Bell TV, a telecommunications company. The Court held that Bell had failed to comply with its obligations pursuant to the *PIPEDA* by conducting a credit check without the plaintiff's prior consent. Prior to this decision, the federal Privacy Commissioner had found that the plaintiff's privacy rights were violated under the *PIPEDA*.

In *Karasik v. Yahoo! Inc.*, 2021 ONSC 1063, the Ontario Superior Court approved a class action settlement against Yahoo! relating to cyberattacks against Yahoo! by unidentified attackers that resulted in the exposure of PI of 5 million Canadians. The issues certified for settlement included negligence in failing to take reasonable steps to establish, maintain, and enforce appropriate security safeguards, and negligence in failing to notify the class members about the incidents. In this decision, the Court undertook a deep analysis of the state of law for privacy class actions. The decision reflects the fact that while most privacy-related class action cases are certified, none have gone to trial and *per capita* settlement amounts tend to be extremely low. As noted by the Court, "it will take a trial decision awarding more than notional-nominal general damages" to change the landscape. Subsequently, in *Larocque v Yahoo! Inc.*, [2022] SJ No. 224, 2022 SKQB 136, the Queen's Bench for Saskatchewan held that the approved class action settlement in Ontario was not meaningfully unfair or that it failed to serve the best interests of the class; it directed a permanent stay of the issue in Saskatchewan.

In *Owsianik v Equifax Canada Co.* [2021] O.J. No. 3171, Equifax Canada Co. and Equifax Inc. ("Equifax") appealed the certification of a class action arising from the breach of a database which exposed the PI of 20,000 Canadians. At the certification hearing, the judge certified a number of causes of action, including intrusion upon seclusion. Equifax challenged whether a claim of intrusion upon seclusion could be brought against a collector or custodian of private information whose property was hacked by a third party. The appeal was allowed. The certification of the class proceeding on the tort of intrusion upon seclusion was set aside. The Ontario Superior Court of Justice (Divisional Court) found that the certification judge erred in finding that the plaintiffs' pleadings disclosed a cause of action for intrusion upon seclusion. This is a significant decision given that the tort was seen as useful tool for data breach class action plaintiffs who would have no practical way of proving individual pecuniary losses. A defendant who collects or holds PI that is accessed by third-party cyber criminals is not liable for intrusion upon seclusion. The Court allowed the class plaintiffs to proceed with their negligence claim, though this may be a pyrrhic victor given the difficulty in demonstrating direct damages.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Yes. In past class action lawsuits, representative plaintiffs have alleged various torts, including negligence in failing to prevent an incident. There have been no trial determinations for privacy class actions in Canada, though settlement approval decisions suggest that grounds exist to award damages on this basis. That said, the *Owsianik* decision, cited above, suggest a possible trend towards a narrowing of the grounds for pursuing organisations that are themselves the victims of third-party cyber criminality.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, organisations are permitted to take out insurance against incidents. Many commercial insurers offer specialised cybersecurity insurance. This can be in the form of third-party liability coverage or first-party expense coverage, or both.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No, there are no regulatory limitations.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. anti-terrorism laws) that may be relied upon to investigate an Incident.

Canada's Privacy Commissioners have broad powers under privacy statutes to investigate complaints, issue reports, compel the production of evidence, issue monetary penalties and make recommendations or initiate audits.

Similarly, the CRTC has a broad range of investigative powers available under *CASL*. In addition to issuing monetary penalties, it may execute search warrants and seize items, as well as obtain injunctions (with judicial authorisation) against suspected offenders.

Local police, provincial police, and the Royal Canadian Mounted Police, along with the national security apparatus (e.g., the CSE and the Canadian Security Intelligence Service) all have broad powers to investigate criminal activities relating to cybersecurity, including terrorism offences, and are granted certain lawful intercept and lawful access rights to private communications under the *Criminal Code* pursuant to prior and valid judicial authorisation.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

No. However, all of Canada's privacy statutes permit an organisation to disclose PI without consent, where the disclosure is to a law enforcement agency in Canada and concerns an offence under Canadian law.

Under the *QC Privacy Law*, an organisation may refuse to communicate PI to the person in respect of whom the information relates, where such disclosure would be likely to hinder an investigation in connection to a crime or a statutory offence, or affect judicial proceedings in which the person has an interest.

Pursuant Section 27(2) of the *CSEA*, the CSE may be authorised by the designated federal minister to access any non-federal infrastructure that is of importance to the government of Canada, and acquire any information originating from, directed to, stored on or being transmitted on or through that infrastructure for the purpose of helping to protect it, in the circumstances described in paragraph 184(2)(e) of the *Criminal Code*, from mischief, unauthorised use or disruption.

Federal Bill C-26 proposes to amend Canada's *Telecommunications Act* and to enact the *Critical Cyber Systems Protection Act*. Under Section 15.5(3), the federal government would be afforded the power to disclose any confidential information it has received from a telecommunications services provider pursuant to an order, where, in the opinion of the government, disclosure is "necessary" to "secure the Canadian telecommunications system, including against the threat of interference, manipulation or disruption". A similar power would be afforded to the government under Section 26(1) of the *Critical Cyber Systems Protection Act*, where, among other reasons, the disclosure of confidential information is "necessary for any purpose related to the protection of vital services, vital systems or critical cyber systems".

Theo Ling is a partner in Baker McKenzie's Intellectual Property & Technology Practice Group. Theo's practice is focused on data and technology-related issues, and digital transformation and data governance initiatives that involve data privacy, data security, electronic payments, data monetisation, records retention, media/format, electronic signatures, cross-border data transfers, digitisation, fintech, and AI and machine learning considerations. Theo also advises clients on internet-related services that involve smart/connected devices, which are subject to regulation under telecommunications and broadcasting laws.

Baker McKenzie
181 Bay Street, Suite 2100
Toronto, Ontario, M5J 2T3
Canada

Tel: +1 416 865 6954
Email: theodore.ling@bakermckenzie.com
URL: www.bakermckenzie.com

Conrad Flaczyk is an associate in Baker McKenzie's Intellectual Property & Technology Practice Group. Conrad's practice focuses on cross-border privacy and cybersecurity matters, including cross-border data transfers, records retention, investigations, and complex cybersecurity breaches. He also advises on regulatory and compliance issues with respect to the roll out of new technologies and consumer-facing offerings, including payment systems, video games, virtual currencies, digital hardware products, mobile apps and other software.

Baker McKenzie
181 Bay Street, Suite 2100
Toronto, Ontario, M5J 2T3
Canada

Tel: +1 416 865 3903
Email: conrad.flaczyk@bakermckenzie.com
URL: www.bakermckenzie.com

Ahmed Shafey is a partner in Baker McKenzie's Litigation and Government Enforcement Practice Group in Canada. Ahmed is known for his focused and practical advice and has had success at all levels of the Court in Ontario as well as with a number of Boards and Tribunals. Ahmed is engaged by clients in a wide range of industries to provide advice in relation to cybersecurity- and data privacy-related concerns and is actively involved in a number of the Firm's innovations in the practice of law.

Baker McKenzie
181 Bay Street, Suite 2100
Toronto, Ontario, M5J 2T3
Canada

Tel: +1 416 865 6964
Email: ahmed.shafey@bakermckenzie.com
URL: www.bakermckenzie.com

John Pirie is a partner in Baker McKenzie's Litigation and Government Enforcement Practice Group in Canada. He is a *Chambers*-listed trial lawyer who acts for clients in complex business disputes, with significant experience in cross-border litigation and arbitration. John has been recognised by *Chambers*, *The Legal 500*, *Benchmark Litigation* and in *L'Expert's Annual Guide to the Leading Canada/US Cross-Border Litigation Lawyers*. John's practice includes a significant fraud and financial crime component. He has appeared as counsel in a number of the country's leading corporate and civil fraud cases.

Baker McKenzie
181 Bay Street, Suite 2100
Toronto, Ontario, M5J 2T3
Canada

Tel: +1 416 865 2325
Email: john.pirie@bakermckenzie.com
URL: www.bakermckenzie.com

Baker McKenzie acts for many of the world's and Canada's largest multinationals, offering first-class domestic and cross-border legal advice on a range of business issues. With over 50 years of experience in the Canadian market, we are committed to helping clients fulfil their ambitions in an increasingly complex global marketplace.

Our Intellectual Property & Technology Practice Group is well known for developing and implementing strategies/programs to help clients efficiently navigate the Canadian and global regulatory landscape, as it pertains to issues that regularly arise across technology verticals. Our lawyers have expertise in a broad range of issues faced by industry participants, including intellectual property protection, data privacy, data security, cross-border data transfers, etc.

Our Litigation team has extensive experience in disputes focused on technology, media and telecommunications issues. Consistently top-ranked by leading market surveys, Baker McKenzie's commercial litigation practice represents clients in complex multi-jurisdictional litigation involving novel and precedent-setting issues.

www.bakermckenzie.com

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

The International Comparative Legal Guides are published by: global legal group