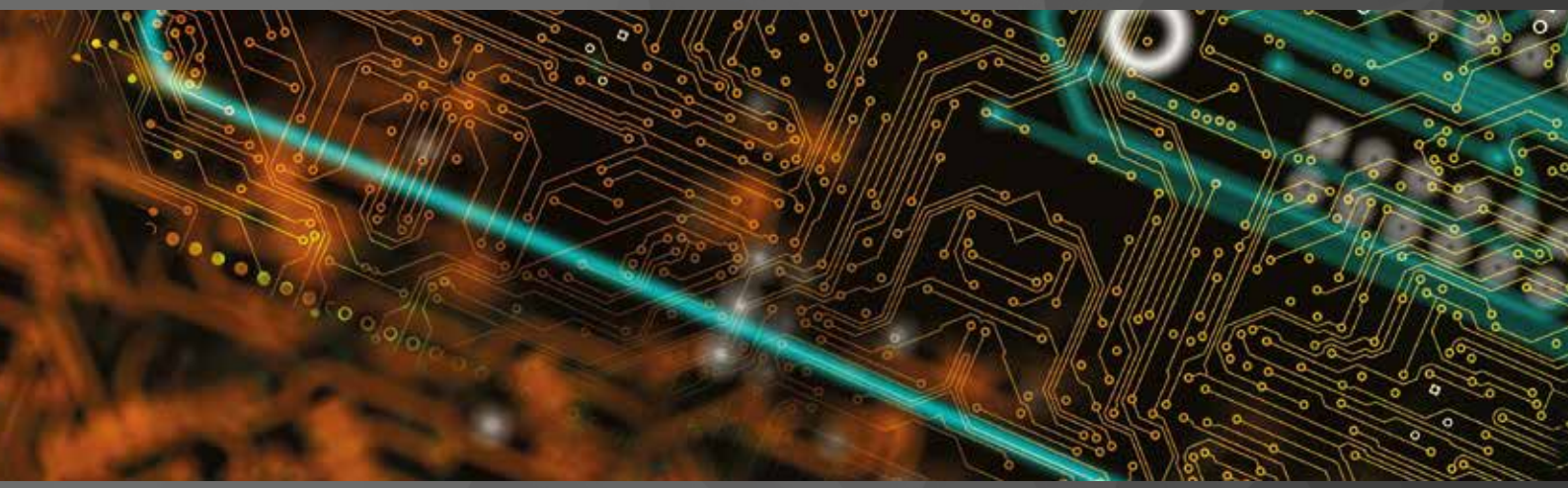
International Comparative Legal Guides



Cybersecurity 2021

A practical cross-border insight into cybersecurity law

Fourth Edition

Featuring contributions from:

Alburhan
Allen & Overy LLP
Ankura Consulting Group
Creel, García-Cuéllar, Aiza y Enríquez
Drew & Napier LLC
Eversheds Sutherland (Germany) LLP
Hamdan AlShamsi Lawyers & Legal Consultants
Ince
Iwata Godo
Kellerhals Carrard
King & Wood Mallesons
Kluge Advokatfirma AS
Lee & Ko
Lee and Li, Attorneys-at-Law
Leśniewski Borkiewicz & Partners (LB&P)
Maples Group
McMillan LLP
Mori Hamada & Matsumoto
Nikolinakos & Partners Law Firm
Nyman Gibson Miralis
Pearl Cohen Zedek Latzer Baratz
R&T Asia (Thailand) Limited
Ropes & Gray LLP
Rothwell Figg
Rubino Avvocati
Schönherr Rechtsanwälte GmbH
Simion & Baciu
Sirius Legal
Stehlin & Associés
TIME DANOWSKY Advokatbyrå AB

ICLG.com

Expert Chapters

Q&A Chapters

Canada


Lyndsay A. Wasser


Kristen Pennington

McMillan LLP

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)
Wilful interception of private communications is a criminal offence under Section 184 of the *Criminal Code of Canada*, RSC 1985, c C-46 (the "**Code**"), with a maximum sentence of five years' imprisonment.

Section 342.1 of the Code prohibits fraudulently obtaining any computer service or intercepting any function of a computer system. Use of a computer system with intent to commit such an offence and use or possession of a computer password to enable such an offence are also prohibited. The maximum sentence is 10 years' imprisonment. The elements of this offence were recently discussed by the Alberta Court of Appeal in *R v. McNish*.

Hacking has also been prosecuted under:

- Section 380(1) of the Code, which prohibits defrauding the public or any person of property, money, valuable security or a service, and carries a maximum penalty of 14 years' imprisonment where the subject matter of the offence exceeds $5,000. In *R v. Kalonji*, the accused was found guilty of fraud and conspiracy to commit fraud in connection with an account take-over scheme involving the hacking of bank accounts.
- Section 430 of the Code, particularly when the hacking is related to "smurfing" (e.g. overloading computer systems causing chaos). In *R v. Geller*, an accused was charged with mischief to data after obtaining credit card numbers and other information through hacking, then accessing the internet using fake identification.

Denial-of-service attacks
Denial-of-service attacks could be considered "mischief" under Section 430(1.1) of the Code, which prohibits obstructing, interrupting or interfering with the lawful use of computer data and denying access to computer data to a person who is entitled to such access. The maximum penalty is 10 years' imprisonment.

Phishing
Phishing may constitute fraud pursuant to Section 380(1) of the Code. In *R v. Usifoh*, the accused was found guilty of receiving funds from various victims of phishing scams.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Section 430 of the Code prohibits "mischief", which includes wilfully destroying or damaging property, rendering property useless, inoperative or ineffective, or obstructing, interrupting or interfering with the lawful use, enjoyment or operation of property. Section 430(1.1) of the Code specifically prohibits wilfully destroying or altering computer data, rendering computer data meaningless, useless or ineffective, obstructing, interrupting or interfering with the lawful use of computer data and denying access to computer data to a person who is entitled to such access. The maximum penalty is 10 years' imprisonment.

Section 8(1) of the *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*, SC 2010, c 23 ("**CASL**") prohibits, during the course of a commercial activity, installing or causing to be installed a computer program on any other person's computer system, unless an owner or authorised user of the computer system consents (subject to certain conditions) or 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
Pursuant to Section 342.2 of the Code, it is illegal to sell or offer for sale a device that is designed or adapted primarily to commit an offence under Section 342.1 (hacking) or Section 430 (mischief).

Possession or use of hardware, software or other tools used to commit cybercrime
Pursuant to Section 342.2 of the Code, it is illegal to make, possess, import, obtain for use, distribute or make available a device that is designed or adapted primarily to commit an offence under Section 342.1 (hacking) or Section 430 (mischief), knowing that the device has been used or is intended to be used to commit such an offence. The maximum penalty is up to two years' imprisonment and/or an order to forfeit the offending device(s).

Identity theft or identity fraud (e.g. in connection with access devices)
Section 402.2 of the Code prohibits obtaining or possessing another person's identity information with the intent to use it to commit an indictable offence such as fraud. The maximum sentence is five years' imprisonment. In *R v. Levesque*, the

accused held multiple forms of identity information, including credit cards and passports. The only reasonable inference the Court could make in the circumstances was that the accused intended to commit fraud or personation.

Fraudulently "personating" another with the intent of gaining an advantage, obtaining property, causing disadvantage to another or to avoid arrest or prosecution is prohibited under Section 403 of the Code. The maximum penalty is 10 years' imprisonment. Personating includes pretending to be the person or using the person's identity information, including their name, signature, username or password. In *R v. Mackie*, the accused was found guilty of personation after gaining access to young peoples' Facebook accounts and pretending to be a victim in order to contact other children.

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

Pursuant to Section 342.1 of the Code, it is an offence to fraudulently obtain, without colour of right, any computer service, including data processing, and the storage or retrieval of computer data. See, for instance, *R v. St-Martin*, where a police officer fraudulently obtained electronic information regarding multiple individuals using a police database.

Section 41.1(1) of the *Copyright Act*, RSC 1985, c C-42 prohibits circumvention of a "technological protection measure", including any technology, device or component that controls access to a work or sound recording or restricts violations of certain copyright provisions. Circumventing a technological protection measure includes descrambling a scrambled work, decrypting an encrypted work or otherwise avoiding, bypassing, removing, deactivating or impairing the technological protection measure without consent. Some violations of Section 41 can lead to fines of up to $1 million, imprisonment for up to five years or both. In *Nintendo of America Inc. v. King*, the respondent was found to have trafficked in circumvention devices for Nintendo's technological protection measures.

Some Data Protection Statutes (as defined in question 2.1) also allow for the imposition of administrative penalties or fines for improperly collecting, using, disclosing, gaining or attempting to gain access to personal information ("**PI**"). For example, pursuant to Section 107 of the *Health Information Act*, RSA 2000, c H-5 (Alberta), a person who knowingly gains or attempts to gain access to health information in contravention of the Act is guilty of an offence and can be fined up to $50,000. Alberta's private sector privacy legislation, the *Personal Information Protection Act*, SA 2003, c P-6.5, also makes it an offence to collect, use, disclose, gain or attempt to gain access to PI in contravention of the Act, subject to a fine of up to $10,000 for an individual and up to $100,000 for a person other than an individual.

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

It is possible that unsolicited penetration testing could be prosecuted under Section 430(1.1) (mischief) and/or Section 342.1 (hacking) of the Code.

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

Pursuant to Section 83.2 of the Code, an individual who commits an indictable offence for the benefit of, at the direction of, or in association with an organisation that commits a terrorist activity is liable to imprisonment for life. Section 83.01 of the Code defines a "terrorist activity" to include an act or omission that intentionally causes serious interference with or disruption of an essential service, facility or system, whether public or private, other than in non-violent protests.

Section 19 of the *Security of Information Act*, RSC 1985, c O-5, makes it an offence to communicate a trade secret with another person, group or organisation, or to obtain, retain, alter or destroy a trade secret, for the benefit of or in association with a foreign economic entity that undermines Canada's economic interests, international relations, or national defence and security. Defences include independent development or reverse engineering, among others. A guilty party may be ordered to serve up to 10 years in prison.

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

Section 6(2) of the Code provides that "no person shall be convicted of an offence that takes place outside of Canada" (see also Section 478(1) of the Code). However, pursuant to Sections 7(3.74) and 7(3.75) of the Code, certain terrorism offences and indictable offences that are considered terrorist activities may be deemed to have been committed in Canada, including when the offence is committed by or against a Canadian citizen.

The Supreme Court of Canada has held that, where a "significant portion" of the activities constituting an offence took place in Canada, a Canadian court may assume jurisdiction. A court will consider whether there is a "real and substantial link" between the alleged crime and the jurisdiction seeking to enforce the law (see *R v. Libman*).

Pursuant to Section 26(1) of the *Security of Information Act*, a person is deemed to have committed an offence in Canada, despite the fact the act or omission took place elsewhere, if the person: is a Canadian citizen; is someone who owes allegiance to Her Majesty in right of Canada; performs functions for a Canadian mission; or returns to Canada after the offence was committed.

Certain provisions of CASL may have extraterritorial application. For example, Section 8 (installation of computer program) applies if the computer system is located in Canada at the relevant time, or if the person is either in Canada at the relevant time or is acting under the direction of a person who is in Canada at the time when they give the directions.

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)?

Sentencing in Canada is determined on a case-by-case basis, relying on statutory guidance under Section 718 of the Code. The basic principle is that the sentence must "be proportionate to the gravity of the offence and the degree of responsibility of the offender" (Section 718.1 of the Code). Additionally, "the degree of planning involved in carrying out the offence and the duration and complexity of the offence" are also considerations (Section 718.21(b) of the Code).

Certain criminal offences require proof of criminal intent (e.g. *mens rea*). Also, some offences may not apply where the action was undertaken with consent. For a recent discussion of intent as it related to Section 430(1.1) (mischief), Section 342.1 (hacking), and Section 24 (attempts) of the Code, see *R v. Livingston*.

The penalties for some offences depend upon the financial repercussions of the offence. For example, Section 380(1) of the Code (see Section 1.1) carries a maximum sentence of 14 years'

imprisonment for fraud involving $5,000 or more, whereas the maximum sentence is reduced to two years' imprisonment if the value of the subject-matter of the offence is less than $5,000. There are also other aggravating factors, such as the number of victims or the complexity of the fraud, that may increase the severity of the punishment (see Section 380.1(1)).

2 Cybersecurity Laws

2.1 *Applicable Law*: 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.

CASL prohibits, in the course of a commercial activity: (a) alteration of the transmission data in an electronic message so that the message is delivered somewhere other than, or in addition to, the destination specified by the sender (Section 7(1)); (b) installation of a computer program on another's computer system without consent (Section 8(1)); and (c) aiding, inducing, procuring or causing any of the above (Section 9). Violations of CASL can result in administrative monetary penalties of up to $1 million per violation by an individual and $10 million per violation by an organisation.

See also question 1.1 for discussion of Section 19 of the *Security Information Act*, which relates to trade secrets.

Canada also has a number of statutes that apply to the protection of PI, including (collectively "**Data Protection Statutes**"):

- the Federal *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 ("**PIPEDA**") applies to the protection of PI handled in the course of commercial activities (except in provinces that have substantially similar legislation), and to the protection of employee PI by federally regulated organisations;
- the Provinces of Alberta, British Columbia and Quebec each have legislation that is substantially similar to PIPEDA, which applies to the protection of PI by private sector organisations within these provinces;
- each Canadian jurisdiction has legislation governing the protection of PI by government bodies/institutions; and
- most provinces have legislation that applies to the protection of personal health information by certain types of custodians, such as doctors and hospitals.

Quebec has proposed significant potential amendments to its privacy laws by tabling Bill 64, *An Act to modernise legislative provisions as regards the protection of personal information* ("**Bill 64**"). Bill 64, if passed, is intended to modernise the province's legislative framework with respect to the protection of PI in both the public and private sectors. Quebec already has in force *An Act to establish a legal framework for information technology*, SQ 2001, c 32, which requires that certain measures be taken to protect confidential information stored in electronic documents and format, and sets out rules governing the use, retention and transmission of electronic data, including biometric information.

As part of the National Cyber Security Strategy, the federal government has released a 10-principle Digital Charter ("**Charter**"), including a "safety and security" principle that represents Canadians' right to rely on the integrity, authenticity and security of the services they use and to feel safe online. Though the Charter does not have the force of law, its principles are intended to guide the government's policy and actions.

Export control laws can also have cybersecurity implications. For example, Canada's Export Control List (the "**ECL**") identifies specific goods and technologies that are controlled for export, including some computer systems, equipment, components and software designed or modified for the generation, command and control or delivery of "intrusion software", as defined in the ECL.

Organisations are also required to comply with any representations they make to the public regarding their handling of PI, including the safeguards taken by the organisation to prevent an Incident. As discussed further at question 2.6, the Competition Bureau can investigate false and misleading statements and representations about consumers' privacy and the handling of their PI.

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

The Communications Security Establishment ("**CSE**") is the technical authority for cybersecurity and information assurance in Canada. Its mandate includes providing advice, guidance and services to ensure the protection of computer networks and electronic information of importance to the Canadian government, including combatting foreign-based cyberattacks on critical infrastructure. The CSE establishes IT security standards, practices and directives for IT security practitioners across the federal government.

Public Safety Canada has issued a document providing a set of recommended security steps for organisations involved in critical infrastructure to implement, in order to combat insider risk of cyberattacks.

The Canadian Centre for Cyber Security has issued alerts notifying health organisations of the increased risk to their cybersecurity in light of the current worldwide pandemic and has provided guidance on key vulnerabilities and mitigation strategies.

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.

The Data Protection Statutes require protection of PI. For example, PIPEDA requires that PI be protected against loss or theft, unauthorised access, disclosure, copying, use or modification. The nature of the safeguards should vary depending on the sensitivity, amount, distribution, format and method of storage of the PI, and should include technological measures such as passwords and encryption.

Some of the Data Protection Statutes contain breach reporting, recording and notification obligations in the event of an Incident that impacts PI, as described further at question 2.5.

Certain industry regulators also require organisations to monitor, detect, prevent and/or mitigate Incidents, including:

- The Canadian Securities Administrators ("**CSA**") has issued several Staff Notices relevant to cybersecurity, including without limitation: Staff Notice 11-326 ("Cyber Security"); Staff Notice 11-332 ("Cyber Security"); Staff Notice 33-321 ("Cyber Security and Social Media"); Staff Notice 11-338 ("CSA Market Disruption Coordination Plan"); and Multilateral Staff Notice 51-347. These Staff Notices address matters such as the CSA's expectations for market participants (e.g. that they adopt a cybersecurity

framework that is appropriate to their size and scale) and the measures firms should take to prevent and respond to Incidents (e.g. implementing preventative practices, adequate and current staff training and a written Incident response plan). Firms are expected to conduct a cybersecurity risk assessment at least annually.

- The Office of the Superintendent of Financial Institutions ("**OSFI**") has issued several publications related to cybersecurity, including the "Cyber Security Self-Assessment Guidance" memorandum for Federally Regulated Financial Institutions ("**FRFI**"), which indicates that FRFI senior management is expected to review cyber risk management policies and practices to ensure that they remain appropriate and effective based on evolving circumstances and risks. OSFI has also published a cybersecurity self-assessment template that it encourages organisations to use and may require an organisation to complete. OSFI's "Guideline B-10" sets out expectations for FRFIs regarding the protection of information disclosed to service providers.
- The Investment Industry Regulatory Organization ("**IIROC**") has released a "Cybersecurity Best Practices Guide", which provides dealer members with a voluntary risk-based cybersecurity framework comprising industry standards and best practices. IIROC's "Cyber Incident Management Planning Guide" assists dealer members in preparing internal response plans for Incidents. IIROC has also recently amended its Dealer Member Rules to mandate certain reporting requirements, which are discussed further at question 2.4.
- The Mutual Fund Dealers Association of Canada ("**MFDA**") has released bulletins on cybersecurity describing sources of threats and providing guidance on creating a cybersecurity framework. The MFDA actively engages with members to identify risks in their cybersecurity practices and provide recommendations for improvements, including pursuant to its Cybersecurity Assessment Program.

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.

Some Data Protection Statutes contain breach reporting and recording obligations in the event of an Incident. For example, PIPEDA 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 PIPEDA. If an Incident gives rise to a real risk of significant harm to any individual(s), the Incident must be reported to the Office of the Privacy Commissioner of Canada ("**OPC**") and the organisation must notify affected individuals and any organisation or government institution that may be able to reduce or mitigate the risk of harm. PIPEDA prescribes the minimum content for reports to the OPC, including (without limitation) a description of the Incident, timing of the Incident, the PI impacted, the number of individuals impacted and the steps taken to mitigate/reduce the risk of harm.

Some of the Data Protection Statutes also contain breach reporting and notification requirements, 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 discussed further at question 5.3, the CSA requires organisations to consider disclosure of cybercrime risks, Incidents and related controls in their prospectus or continuous disclosure filings. In addition, regulated exchanges, marketplaces, clearing agencies and alternative trading systems may be subject to Incident reporting requirements under recognition or exemption orders issued by various CSA jurisdictions, including those set out in Instruments NI 21-101, NI 23-101 and NI 24-102. Many exchanges, marketplaces and clearing agencies are required to promptly notify the CSA of a material systems issue, security breach or system intrusion. The CSA also expects that systematically important clearing agencies and settlement systems will inform the Bank of Canada of a market disruption event.

OSFI's "Technology and Cyber Security Incident Reporting" memorandum requires that an Incident be reported to OSFI when it could materially impact the normal operations of a FRFI (including the confidentiality, integrity or availability of its systems and information) and is assessed to be of a high or critical severity level. The memorandum lists characteristics of reportable Incidents and requires reporting to OSFI (including certain specified information) as soon as possible, but no later than 72 hours after it is determined that the Incident is reportable. FRFIs have an ongoing obligation to provide updates to OSFI as new information becomes available.

IIROC amended its Dealer Member Rules in November 2019 to require mandatory reporting of Incidents where: there has been or there is a reasonable likelihood of substantial harm to any person or a material impact on the Dealer's operations; the Dealer invokes a business continuity or disaster recovery plan; or there is a requirement to notify any government body or regulatory authority. Dealers must file an initial report with IIROC describing the Incident within three calendar days of its discovery. Within 30 days of the Dealer's discovery of an Incident, a more detailed report outlining their findings in the course of their investigation must be submitted.

The MFDA requires that members report any breach of client confidentiality, including as a result of a cyberattack.

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.

Some of the Data Protection Statutes contain notification obligations in the event of an Incident that impacts PI. For example, PIPEDA requires that individuals be notified of any breach of security safeguards involving PI under the organisation's control, as soon as feasible, if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual.

PIPEDA prescribes the content and manner of delivering the notice. The notice must contain sufficient information to allow individuals to understand the significance of the Incident

to them and to take steps to reduce/mitigate the risk of harm, and must contain certain prescribed content, including (without limitation) a description of the Incident, timing of the Incident, the PI impacted and the steps taken by the organisation to mitigate/reduce the risk of harm.

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

Compliance with PIPEDA is generally enforced by the OPC; however, certain offences can be prosecuted by the Attorney General ("**AG**"). Each province has a regulator responsible for enforcing the relevant provincial Data Protection Statutes.

CASL is enforced by the Canadian Radio-television and Telecommunications Commission ("**CRTC**"), the OPC and the Competition Bureau.

The Competition Bureau also has jurisdiction to investigate false and misleading statements and representations about consumers' privacy and the handling of their PI, including how such PI is maintained, pursuant to its authority under the *Competition Act*, RSC 1985, c C-34.

See, also, the industry-specific regulators described in question 2.3, which oversee compliance with their cybersecurity policies, guidelines and industry-specific Applicable Laws.

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

The OPC can make non-binding recommendations in the event of non-compliance with PIPEDA and, following the OPC's decision, an application can be made to the Federal Court for damages to complainants. The AG can prosecute an organisation for failure to comply with the breach reporting, notification and recording obligations under 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 also provide for fines in the event of non-compliance.

Organisations that violate the *Competition Act* by making a false or misleading representation to the public in a material respect, including with respect to consumers' privacy and the handling of their PI, can be subject to penalties of up to $10 million for a first offence, and up to $15 million for subsequent offences.

Criminal offences and failure to comply with CASL carry the penalties as described in questions 1.1 and 2.1.

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

The OPC has investigated a number of Incidents involving breaches of PI, including:

- PIPEDA Report of Findings #2016-005 – Investigation of Ashley Madison in connection with hacking and online posting of users' account information (resulted in recommendations by the OPC);
- PIPEDA Report of Findings #2019-001 – Investigation into Equifax after an attacker accessed sensitive PI of customers (resulted in a compliance agreement);
- PIPEDA Report of Findings #2018-001 – Investigation into VTech Holdings Limited following the potential compromise of PI respecting over 553,000 Canadians, including children's names, genders, dates of birth, pictures, voice recordings and chat discussions with parents;
- PIPEDA Report of Findings #2007-389 – Investigation into TJX after a network computer intrusion affected payment card information; and
- PIPEDA Report of Findings #2018-006 – Investigation into the World Anti-Doping Agency following a breach of its database, which resulted in the public disclosure of the PI of Olympic athletes.

The CRTC has also taken enforcement action under CASL, including against Datablocks Inc. (fine of $100,000) and Sunlight Media Network Inc. (fine of $150,000) for violations of Sections 8 and 9 of CASL. The CRTC found that advertisements distributed through the companies' services resulted in the unlawful installation of malicious programs on computer systems by third parties, and that neither company took appropriate steps to prevent such CASL breaches, thereby aiding the violations.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction?

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)

Organisations subject to the Data Protection Statutes are generally required to provide notice and/or obtain consent to the collection and use of PI. The OPC considers metadata collected using beacons to be PI and has indicated that organisations should not undertake types of web tracking that individuals cannot stop or control without taking extraordinary measures (or at all), as these forms of tracking do not allow for individuals to consent or withdraw consent, contrary to PIPEDA.

It is possible that beacons used only for data security purposes may fall within the exceptions to notification and/or consent requirements under the applicable Data Protection Statute(s). However, a specific evaluation of Applicable Laws in the relevant jurisdiction(s) should be undertaken.

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 by Applicable Laws. However, to the extent the honeypot involves the collection, use or disclosure of PI, notice and consent considerations may apply. Honeypots may be problematic under CASL, depending upon the manner in which they operate.

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 by Applicable Laws. However, to the extent the sinkhole involves the collection, use or disclosure of PI, notice and consent considerations may apply. Compliance with CASL should also be considered.

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?

Such monitoring or interception would generally be permissible,

provided it is reasonable and complies with the requirements of any applicable Data Protection Laws, and provided the organisation has a "colour of right" pursuant to Section 342.1 of the Code (hacking). Advance notice/consent in a form prescribed by Data Protection Laws may be required. Monitoring of employees in a unionised workplace raises additional concerns that should be evaluated on a case-by-case basis for compliance with any applicable collective agreement(s). Organisations should consult local counsel in the relevant jurisdiction(s) to ensure full compliance with all Applicable 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?

Canadian export controls' limitations vary in scope depending on the type of product and its ultimate destination. Canada controls the flow of encryption items out of the country through the *Export and Import Permits Act*, RSC 1985, c E-19, Group 1, Category 5 – Part 2: Information Security. Cryptography falls under the "Dual-Use List", as encryption products can be used for military purposes as well as civil and commercial applications. Exceptions to the export controls may apply for certain countries under a General Export Permit. See, for instance, *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.

Many organisations in various industries have recognised that compliance with statutory requirements should not be the end goal for data protection and have voluntarily committed to a higher standard. Examples include, without limitation, the telecommunications and financial services industries, as well as service providers to healthcare institutions and government institutions/bodies. Payment processors in Canada also typically comply with the Payment Card Industry Data Security Standard (PCI-DSS).

4.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Organisations in the financial services and telecommunications sectors must comply with PIPEDA, including (in many cases) with respect to employee PI. See Section 2 for additional requirements applicable to the financial sector, including pursuant to OSFI's guidance documents.

The Bank of Canada, Department of Finance and OSFI have also collaborated with G-7 partners to publish the following guidelines: (a) G-7 Fundamental Elements of Cybersecurity for the Financial Sector; (b) G-7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector; and (c) G-7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector.

The Canadian Security Telecommunications Advisory Committee has developed Security Best Practices for telecommunications service providers that supply and support Canada's telecommunications critical infrastructure. These voluntary practices include ongoing security testing, network security monitoring, Incident response capabilities and developing breach notification procedures.

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?

Directors' and officers' personal liability with respect to Incidents has not been expressly considered by Canadian courts. However, directors and officers can be held liable for breaches of fiduciary duties if they fail to: act honestly and in good faith with a view to the best interests of the company; or exercise the care, diligence and skill of a reasonably prudent person in comparable circumstances. Therefore, failure to take steps to address cybersecurity concerns of which the director or officer was aware (and that a reasonable person would have remedied) could potentially expose them to personal liability. A due diligence defence may apply if the director or officer relied in good faith on statements, documents and reports created by professionals.

There may also be a risk of personal liability if directors and officers misrepresent the organisation's cybersecurity measures, fail to disclose cybersecurity risks or Incidents in annual reporting (if applicable), or are otherwise untruthful or careless about cybersecurity Incidents or risks.

Directors and officers may also be held personally responsible for violations of certain statutes at the federal and provincial level. For example, pursuant to Section 31 of CASL (subject to a defence of due diligence), an officer, director, agent or mandatary of a corporation may be liable if they directed, authorised, assented to, acquiesced in, or participated in the commission of a violation of the Act.

Pursuant to Section 93 of Quebec's *Act respecting the protection of personal information in the private sector*, a director or representative of a corporation is liable as a party to an offence if it is found that the corporation committed an offence and the director ordered or authorised the act or omission constituting the offence. For the first offence, fines range between $1,000 and $10,000 for anyone who collects, holds, communicates to third parties, or uses PI for purposes contravening the Act. Fines increase with repeated offences (see Section 91).

Under some provincial health privacy legislation, a director or officer may be liable as a party to a corporation's offence if they authorised the offence or could have prevented the offence from being committed and knowingly did not do so.

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?

Some federal and provincial privacy statutes require organisations to designate a person responsible for compliance with the applicable legislation. For example, PIPEDA Schedule 1, Principle 4.1 requires designation of one or more individual(s) who are accountable for compliance with the PIPEDA principles, including those set out under Principle 4.7, "Safeguards".

Guidance documents and findings in prior cases published by the OPC and other regulators indicate that all organisations should have a written Incident response plan/policy, and should conduct periodic cyber risk and vulnerability assessments, as well as penetration tests. Failure to do so would typically be considered non-compliant with the organisation's general obligations to protect information under the Applicable 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)?

As discussed in question 2.4, some institutions are required to disclose cybersecurity risks or Incidents as part of their prospectus or ongoing disclosure obligations. Factors relevant to assessing disclosure obligations include the probability that an Incident will occur and the anticipated magnitude of its effects. The issuer is expected to provide disclosure that is detailed and entity-specific. In addition, regulated exchanges, marketplaces, clearing agencies and alternative trading systems may be subject to Incident reporting requirements under recognition or exemption orders issued by various CSA jurisdictions, including those set out in Instruments NI 21-101, NI 23-101 and NI 24-102.

The CSA's Multilateral Staff Notice 51-347 ("Disclosure of cybersecurity risks and incidents"), a joint publication of the British Columbia Securities Commission, the Ontario Securities Commission and Quebec's Autorité des marchés financiers, provides that issuers must undertake a contextual analysis when determining whether and when an Incident constitutes a material fact or material change that requires disclosure in accordance with securities legislation. Issuers are expected to address in their Incident remediation plans for how an Incident will be assessed to determine whether, what, when and how the Incident will be disclosed.

Some laws of general application and/or specific sectoral or provincial laws have requirements that are relevant to cybersecurity (e.g. Quebec's *An Act to Establish a Legal Framework for Information Technology*). Organisations should consult local counsel in the relevant jurisdiction(s) to ensure full compliance with all Applicable Laws.

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.

It is common for class action lawsuits to be filed in Canada following an Incident involving the breach of PI. Representative plaintiffs commonly allege negligence, intrusion upon seclusion, breach of fiduciary duty, breach of contract, breach of warranty, breach of confidence, violation of privacy, publicity given to private life/public disclosure of private facts, breach of consumer protection legislation and/or conspiracy.

With respect to a claim of negligence, a plaintiff would generally have to prove the existence of a duty of care, breach of the standard of care, causation, and damages.

With respect to the tort of intrusion upon seclusion, the test requires proof on an objective standard that the alleged invasion of privacy would be highly offensive to a reasonable person.

With respect to a claim for breach of a fiduciary duty, a plaintiff would first have to prove the existence of a fiduciary relationship, then show that the fiduciary breached its obligations with respect to the fiduciary relationship by doing something that is contrary to the plaintiff's interests.

To make out a claim for breach of contract or breach of warranty, a plaintiff would have to show the existence of a valid and binding contract between the parties, a breach of the terms of the contract, and damages as a result of such breach. A breach of warranty typically entitles a successful plaintiff exclusively to damages.

With respect to a claim of breach of confidence, proof that the information was confidential, that it was communicated in confidence, and that it was misused by the recipient of the communication is required.

With respect to the tort of public disclosure of private facts, a plaintiff must prove that the disclosure was public, that the facts disclosed were private, and that the matter made public or the act of the publication would be highly offensive to a reasonable person and not of legitimate concern to the public.

The tort of simple motive conspiracy generally requires a plaintiff to show that the defendant engaged in conduct with the predominant purpose of causing the plaintiff injury, and that this conduct resulted in injury to the plaintiff.

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.

Some examples of class action lawsuits filed in connection with Incidents include:

- *Kaplan v. Casino Rama*, 2019 ONSC 2025 – Alleging that Casino Rama breached its privacy policy by failing to take reasonable security measures to protect against unauthorised access to class members' personal and confidential information.
- *Lozanski v. The Home Depot Inc.*, 2016 ONSC 5447 – Regarding a payment card system hacked by criminal intruders using custom-built malware.
- *Drew v. Walmart Canada Inc.*, 2017 ONSC 3308 – Following the breach of an online photo centre operated by a third-party service provider.
- *Tucci v. Peoples Trust Company*, 2017 BCSC 1525 – Alleging breach of contract, confidence and privacy, negligence and intrusion upon seclusion or, in the alternative, unjust enrichment and waiver of tort regarding a compromised database.
- *Maksimovic v. Sony of Canada Ltd.*, 2013 CanLII 41305 – Following a cyber-attack resulting in access to account holder information.
- *Zuckerman v. Target Corporation*, 2017 QCCS 110 – Regarding a breach affecting payment card data, including name and credit/debit card number, expiration date and security code.
- *Dentons Canada LLP v. Trisura Guarantee Insurance Company*, 2018 ONSC 7311 – Regarding a social engineering fraud, which resulted in a lawyer mistakenly transferring client funds to a fraudulent account.
- *Bourbonnière c. Yahoo! Inc.*, 2019 QCCS 2624 – Regarding stolen PI and financial information caused by various Incidents experienced by Yahoo!.
- *Del Giudice v. Thompson*, 2020 ONSC 2676 – Regarding an Incident which resulted in unauthorised access to the PI of those who applied for credit products.

Class action lawsuits were also filed in connection with the Incidents experienced by Ashley Madison and Equifax (see question 2.8).

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

As indicated above, it is common in Canada for class action lawsuits to be filed following an Incident. Representative plaintiffs have alleged various torts, including negligence and privacy torts, such as intrusion upon seclusion. As none of these cases have yet proceeded to trial (although some have settled), the liability of organisations that experience an Incident is still unsettled law in Canada.

7 Insurance

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

Yes. Many general commercial liability policies do not cover Incidents, but specialised cyber risk policies are available and typically tailored to an organisation's particular risk profile as well as its size. Policies vary from first-party coverage, which protects the policy holder, to third-party coverage, which protects the policy holder from third-party claims.

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 not.

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. antiterrorism laws) that may be relied upon to investigate an Incident.

The Canadian government has broad powers to investigate criminal activities, including terrorism offences. For example, Section 487 of the Code permits searches of computer systems, and generation and seizure of data printouts, and allows a court to order the preservation of computer data in some circumstances.

The *Canadian Security Intelligence Service Act*, RSC 1985, c C-23 allows the Director of Service or a designate to seek a warrant triggering broad powers to investigate a threat to Canadian security, both within and outside of Canada.

In connection with the federal government's National Cyber Security Strategy, the Royal Canadian Mounted Police ("**RCMP**") have established the National Cybercrime Coordination Unit ("**NC3**"). The NC3, once fully operational, will coordinate cybercrime investigations and provide investigative advice to law enforcement across Canada.

Regulators that are responsible for enforcing the Applicable Laws described in Section 2 (e.g. the OPC and the CRTC) also have broad investigatory powers. For example, the OPC can, amongst other powers: (a) summon and enforce the appearance of persons and compel them to give oral or written evidence on oath and to produce records in the same manner and to the same extent as a superior court of record; and/or (b) at any reasonable time, enter any premises (except a dwelling house), and converse in private with any person or examine or obtain copies/extracts from records found in such premises.

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, currently there are none.

Lyndsay A. Wasser is the Co-Chair of McMillan's Privacy & Data Protection Group and its Cybersecurity Group. She is a Certified Information Privacy Professional/Canada and regularly advises and assists clients on a broad range of privacy and cybersecurity issues, including advising on legal requirements related to data security, workplace privacy issues, handling personal health information and transferring personal information across borders. She assists clients to develop privacy compliance programmes and data sharing agreements. She has assisted many clients with responding to privacy and data breaches involving various types of information (e.g., payment card information, patient data, employee personal information and sensitive identity information), including assisting with risk assessment, breach response strategy, notification obligations and communications with regulators. Lyndsay regularly writes and speaks on cybersecurity topics and is the co-author of *Privacy in the Workplace*, 4th ed. and the Privacy chapter in the *Ultimate Corporate Counsel Guide*.

McMillan LLP
Brookfield Place, Suite 4400
181 Bay Street, Toronto
Ontario, M5J 2T3
Canada

Tel: +1 416 865 7083
Fax: +1 416 865 7048
Email: lyndsay.wasser@mcmillan.ca
URL: www.mcmillan.ca

Kristen Pennington is an Associate Lawyer in the Toronto office of McMillan, where she practises both privacy and employment law. Kristen advises organisations with respect to legal requirements related to data security and workplace privacy issues, including employee background checks, the processing of personal information in connection with coronavirus, and cross-border transfers of personal information. She assists clients with developing practical, up-to-date privacy compliance programmes and with drafting appropriate data sharing terms with service providers and other third parties. Kristen regularly writes and speaks about emerging Canadian privacy topics and has been featured in a variety of leading industry publications.

McMillan LLP
Brookfield Place, Suite 4400
181 Bay Street, Toronto
Ontario, M5J 2T3
Canada

Tel: +1 416 865 7000
Fax: +1 416 865 7048
Email: kristen.pennington@mcmillan.ca
URL: www.mcmillan.ca

McMillan is a leading Canadian business law firm with recognised expertise and acknowledged leadership in major business sectors, which provides solutions-oriented legal advice through our offices in Vancouver, Calgary, Toronto, Ottawa, Montréal and Hong Kong. McMillan's privacy, data protection and cybersecurity experts have a thorough understanding of legal and regulatory obligations related to cybersecurity, and regularly assist organisations to proactively address and effectively respond to rapidly evolving cyber threats, including by: drafting security and data protection policies and protocols; drafting and reviewing insurance policies addressing cyber risk; negotiating agreements with third party suppliers and service providers to analyse cyber risk implications; advising on compliance with applicable data protection laws and other legislation; strategic handling of data breaches; and advising on and defending claims related to data protection, including defending class action litigation.

www.mcmillan.ca

ICLG.com

Other 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
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
Outsourcing
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
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

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