Privacy and cybersecurity in Canada

Author(s): John Salloum, Rachel St. John, Patricia Kosseim

Getting the Deal Through: Market Intelligence provides a unique perspective on the evolving legal and regulatory landscapes in major jurisdictions worldwide. Recently, the online publication featured Osler lawyers Patricia Kosseim, John Salloum and Rachel St. John in a wide-ranging Q&A that covers many aspects of the current privacy and cybersecurity landscape in Canada. In this in-depth discussion, they address many topics, including:

- the key regulatory developments concerning cybersecurity standards in Canada
- the issues that companies must address when they suffer a data security incident
- the rules surrounding notifying regulators and consumers about data breaches
- the data security and privacy concerns that businesses should consider when thinking about moving data to a cloud-hosting environment
- the best practices Canadian organizations are following to improve cybersecurity preparedness
- the ways the Canadian government is addressing serious cybersecurity threats and criminal activity
- how companies should factor privacy and data security risks into their decision-making when contemplating M&A deals

AN INTERVIEW WITH PATRICIA KOSSEIM, JOHN SALLOUM AND RACHEL ST JOHN

GTDT: WHAT WERE THE KEY REGULATORY DEVELOPMENTS IN YOUR JURISDICTION OVER THE PAST YEAR CONCERNING CYBERSECURITY STANDARDS?

Patricia Kosseim: There have been several recent regulatory developments in Canada in the area of cybersecurity. Most notably: (1) proposed legislation to strengthen the national security regime in Canada, (2) the introduction of new breach notification regulations at the federal level, and (3) key investigation findings issued by the Office of the Privacy Commissioner of Canada.
Bill C-59, An Act respecting National Security Matters was introduced in Parliament in 2017. Among its many provisions, would be a broadened mandate of the Communications Securities Establishment (CSE). Under the proposed law, CSE would have expanded authorities to allow it to interfere with foreign online efforts that threaten Canada, including by protecting Canada’s networks from foreign cyber threats – both defensively and actively. The latter would include degrading, disrupting, influencing, responding to or interfering with the capabilities, intentions or activities of a foreign actor. CSE would also have greater ability to defend critical cyber-infrastructure in the private sector by removing legal barriers to the sharing of certain cyber threat information, the provision of mitigation advice and the deployment of CSE’s cybersecurity tools, upon request. By the same token, however, CSE would also be subject to more robust oversight to keep the exercise of its powers in check, including a strengthened Ministerial Authorization regime and a newly created National Security and Intelligence Review Agency and Intelligence Commissioner. Bill C-59 has been through various Committee hearings over the past year where it underwent several amendments in the House of Commons, and was still working its way through the legislative process in the Senate at the time of writing (August 2018).

Also at the Federal level, new breach notification regulations were introduced pursuant to the Personal Information and Electronic Documents Act (PIPEDA), S.C. 2000, c.5. These regulations are set to come into force, together with the related statutory provisions, on 1 November 2018. The new federal breach notification regime will require private sector organisations subject to PIPEDA to promptly report data breaches above a certain threshold to the Privacy Commissioner and to individuals affected, as well as to notify other organisations or government institutions that may be able to reduce the risk of harm resulting from the breach. The new breach notification rules will also require organisations to maintain, in prescribed form, records of every breach of security safeguards involving personal information under its control. An organisation that knowingly fails to report breaches to the Privacy Commissioner, notify an affected individual, or maintain breach records, as required by law, commits an offence and could be liable for a fine not exceeding C$10,000 in the case of an offence punishable on summary conviction or C$100,000 for an indictable offence.

In terms of regulatory guidance, the Office of the Privacy Commissioner of Canada (OPC) released in January 2018 its investigation findings in the matter of Vtech Holdings (PIPEDA #2018-001, ‘investigation report’). In it, the OPC reiterated the reasonableness standard to which accountable organisations will be held in terms of security safeguards. Although PIPEDA does not require absolute impenetrability against risk of breach, it does require organisations to adopt physical, organisational and technological safeguards appropriate to the sensitivity of the personal information in question.

This case involved a global data breach, involving sensitive personal information of over half a million Canadians, including children. Following an extensive investigation into the matter, the OPC found several safeguard deficiencies, particularly given the sensitivity of the data involved in the breach and the risk of harm that could result therefrom. The safeguarding shortfalls included: ‘(i) a lack of testing and maintenance to identify and mitigate vulnerabilities [...]'; (ii) inadequate administrative access controls; (iii) various cryptographic deficiencies; (iv) the absence of security monitoring and logging to detect potential threats; and (v) no overarching comprehensive security management program’.

As a result, the OPC recommended, and Vtech adopted, the following remedial measures to strengthen its cybersecurity management programme (see paragraph 24 of the investigation report):

(1) adopt a regular, multi-faceted testing protocol and an update/patch management programme to identify and mitigate system vulnerabilities;
(2) limit the number of authorised individuals with administrative-level access controls, strengthen authentication methods through strong passwords and implement organisational measures to strictly control the use of administrative accounts;

(3) enhance cryptographic methods for encrypting stored information and user information in transit between its website and apps;

(4) centralise event logs and monitor activities on the network, including outgoing traffic to the internet, in order to detect and investigate any unauthorised activities;

(5) implement a new comprehensive data security policy with proper governance to ensure among other things:

(i) the creation of a Data Security Governance Board;

(ii) annual staff training regarding the policy and data security;

(iii) compliance with the data security policy;

(iv) annual risk assessments, best-practice benchmarking and reviews so that the policy and associated data security measures remain adequate.

GTDT: WHEN DO DATA BREACHES REQUIRE NOTICE TO REGULATORS OR CONSUMERS, AND WHAT ARE THE KEY FACTORS THAT ORGANISATIONS MUST ASSESS WHEN DECIDING WHETHER TO NOTIFY REGULATORS OR CONSUMERS?

PK: Under PIPEDA's new breach notification regime (Breach of Security Safeguards Regulations, SOR/2018-64), set to come into force on 1 November 2018, organisations will be required to report to the Privacy Commissioner, and to notify affected individuals of, any breach of security safeguards that meets the legally prescribed threshold.

‘Breach of security safeguards’ means ‘the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organisation’s security safeguards ... or from a failure to establish those safeguards’.

Legal threshold

The legal threshold for reporting to the Commissioner and notifying affected individuals is the same, namely: ‘if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual’.

In determining whether a real risk of significant harm exists, organisations must take into account:

(1) the sensitivity of the personal information involved in the breach;

(2) the probability that the personal information has been, is being or will be misused; and

(3) any other prescribed factor (at time of writing, there was no other prescribed factor).

Significant harm includes ‘bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the
credit record and damage to or loss of property’.

Timing

In terms of timing, both the report to the Commissioner and the notification to affected individuals must be made ‘as soon as feasible after the organisation determines that the breach has occurred’.

“Organisations will also come under a positive obligation to maintain a record of every breach of security safeguards.”

Form and content of the Report to the Commissioner

The report to the Commissioner shall be sent in writing, by any secure means of communication, and shall contain the following prescribed elements:

(1) a description of the circumstances of the breach and, if known, the cause;
(2) the day on which, or the period during which, the breach occurred or, if neither is known, the approximate period;
(3) a description of the personal information that is the subject of the breach to the extent that the information is known;
(4) the number of individuals affected by the breach or, if unknown, the approximate number;
(5) a description of the steps that the organisation has taken to reduce the risk of harm to affected individuals that could result from the breach or to mitigate that harm;
(6) a description of the steps that the organisation has taken or intends to take to notify affected individuals of the breach; and
(7) the name and contact information of a person who can answer, on behalf of the organisation, the Commissioner’s questions about the breach.

Form and content of the notification to individuals

The required notification to affected individuals shall contain the following content:

(1) a description of the circumstances of the breach;
(2) the day on which, or period during which, the breach occurred or, if neither is known, the approximate period;
(3) a description of the personal information that is the subject of the breach to the extent that the information is known;
(4) a description of the steps that the organisation has taken to reduce the risk of harm that could result from the breach;
(5) a description of the steps that affected individuals could take to reduce the risk of harm that could
result from the breach or to mitigate that harm; and

(6) contact information that the affected individual can use to obtain further information about the breach.

The notification shall be given to affected individuals directly (that is, in person, by telephone, mail, email or any other form of communication that a reasonable person would consider appropriate in the circumstances).

In limited circumstances, individuals can be notified indirectly (for example, by means of public communication or other reasonable measure expected to reach them) where:

(1) direct notification would be likely to cause further harm to the affected individual;

(2) direct notification would be likely to cause undue hardship for the organisation; or

(3) the organisation does not have contact information for the affected individual.

Other provisions of note

Organisations shall also notify, as soon as feasible after it determines the breach has occurred, any other organisation or government institution that it believes may be able to reduce or mitigate the risk of harm that could result from the breach.

Under Canada’s new breach notification regime, organisations will also come under a positive obligation to maintain a record of every breach of security safeguards and produce such records to the Privacy Commissioner of Canada upon request.

As mentioned above, an organisation that knowingly fails to report breaches to the Privacy Commissioner, notify an affected individual, or maintain breach records, as required by law, commits an offence and could be liable for a fine not exceeding $10,000 in the case of an offence punishable on summary conviction or $100,000 for an indictable offence.

“\textit{The timeline for notifying is short, namely ‘as soon as feasible’ after the organisation learns of the breach.”}"

\textbf{GTDT: WHAT ARE THE BIGGEST ISSUES THAT COMPANIES MUST ADDRESS FROM A PRIVACY PERSPECTIVE WHEN THEY SUFFER A DATA SECURITY INCIDENT?}

\textbf{PK:} When a data security incident occurs, and the race is on to contain potential damage, there is very little time to react on the spot, let alone think about it. To mitigate risks effectively, issues must be anticipated and thought through well beforehand in the form of a robust breach incident readiness and response plan, and its implementation should be pilot-tested several times (through table top exercises for example) to make sure that all of its component parts work well upon deployment. (See more about an effective breach incident readiness and response plan, below.)

Be that as it may, when the time comes, there are no more dress rehearsals. Some of the most
challenging issues that arise in the ‘heat’ of a breach incident involve the preliminary investigation phase. Trying to find the source of the breach and contain the data leak as quickly as possible can be extremely challenging. Sometimes, the problem can be identified and immediately acted upon, for example, by recuperating the lost documents or hard drives, changing passwords, patching infected software, immediately closing off access to company servers, segregating compromised data from the rest of the networks, etc. Other times, the source of the data loss cannot be determined. Suspicious patterns of network behaviour may never be resolved; ransomware may or may not turn out to be empty threats; imposters behind social engineering ploys may never be identified; and missing documents, hard drives or other mobile devices may never be found.

Meanwhile, and at the same time, organisations are expected to gather concrete facts to determine the nature and scope of the information that was breached, its level of sensitivity, the numbers of individuals involved, whether or not it was adequately encrypted, etc. so as to meaningfully assess whether the threshold for notifying data protection regulators and individuals has been met. The timeline for notifying is short, namely ‘as soon as feasible’ after the organisation learns of the breach, failing which the organisation may face stiff penalties. While the temptation may be to notify peremptorily just in case, doing so before all the facts are known risks unduly alarming individuals.

Once a determination has been made that regulators and individuals should be notified, the challenge is in deciding what to say and when, for the situation may be rapidly evolving. Organisations may want to provide as many facts as possible in an effort to be transparent and project a sense of certainty, predictability and control over the situation, yet on the other hand, having to go back on information previously given as one uncovers additional and potentially contradictory facts, risks affecting credibility and may potentially come up in an eventual regulatory investigation, should it come to that.

After the what and when, comes the how. How should individuals be notified? In an effort to help mitigate potential damage, well-meaning organisations may inadvertently jump the gun by wanting to get the information out there as quickly as possible, without sufficient regard to the mechanism for doing so. Sometimes, direct notification to individuals in ways that may inadvertently disclose sensitive personal information about affected individuals to others (family members, roommates, co-workers, etc) may not be appropriate when it risks causing more harm than good. Canadian law explicitly recognises that indirect notification (through public notice) may be an acceptable alternative where appropriate, and organisations will need to carefully think that through.

Along the same vein, well-meaning organisations may rush to offer credit monitoring services by immediately contracting credit monitoring companies to provide these services to affected individuals in an effort to help mitigate harm, while omitting the necessary prior step of seeking individuals’ consent. And in the case minors among the group of affected individuals, that process of contacting and obtaining consent, may add an additional dimension of complexity.

Many times, these issues may be playing themselves out in real time, through the media. Organisations would be well served by having public relations experts on hand, well-steeped in managing crisis communications, ready to go when the need arises. This expertise may be drawn internally, or may be engaged through an external firm on retainer. Organisations should expect to face tensions between what the public relations firms may recommend is best to communicate from a reputational perspective, and what the lawyers may be advising from a potential liability point of view.

In major breach situations, where the prospect of litigation looms, including potential class action lawsuits, and counterclaims against potentially negligent processors, there is a whole additional layer of
challenges facing organisations as they must strive to maintain solicitor-client privilege and preserve the chain of evidence in a volatile and rapid-fire context. Where there are potential criminal elements at play, including malicious hackers, ransomware and possible state-sponsored attacks to critical infrastructure, organisations may find themselves over their heads in dealing with what can be frightening situations. Organisations will have to handle these situations with special caution and know when to reach out to law enforcement and/or other government institutions for assistance.

“Canadian law explicitly recognises that indirect notification (through public notice) may be an acceptable alternative where appropriate.”

**GTDT: WHAT BEST PRACTICES ARE ORGANISATIONS WITHIN YOUR JURISDICTION FOLLOWING TO IMPROVE CYBERSECURITY PREPAREDNESS?**

**Rachel St John:** As a best practice, many organisations doing business in Canada are developing comprehensive cybersecurity plans that expressly contemplate incident preparedness and response. These plans are highly tailored and set out core roles and responsibilities within an organisation. They necessarily involve a detailed preparation exercise to address organisation-specific data and risks.

Some of the critical issues that these cybersecurity plans address include:

- Identifying core roles and responsibilities within an organisation, including the business function that will play the role of response coordinator.
- Setting out strategies for maintaining legal privilege with respect to communications and documentation in respect of an incident.
- Allocating responsibility for maintaining accurate, complete and current records regarding the incident and decisions made with respect to response.
- Illustrating relevant incident containment and investigation steps that align with risks specific to the organisation.
- Identifying notification and reporting obligations in applicable jurisdictions, including breach reporting requirements for affected individuals and regulatory authorities as set forth under Canadian privacy laws.
- Planning for communications and stakeholder relations in the event of an incident.

Once a plan has been developed, organisations should regularly conduct tabletop tests as a means of training to respond to a cybersecurity incident, as well as to identify any gaps or areas for potential improvement in the plan.

“Even the best confidentiality agreements cannot override the local laws of a foreign jurisdiction, including laws related to law enforcement and national security.”
GTDT: ARE THERE SPECIAL DATA SECURITY AND PRIVACY CONCERNS THAT BUSINESSES SHOULD CONSIDER WHEN THINKING ABOUT MOVING DATA TO A CLOUD-HOSTING ENVIRONMENT?

John Salloum: Canadian private sector privacy laws set out fairly consistent obligations for private sector organisations that outsource the processing of personal information. These requirements are generally contained within the statutory-based principles of accountability, safeguards and openness.

Accountability

Under Canada’s federal private sector privacy law (The Personal Information Protection and Electronic Documents Act, or PIPEDA), an ‘organisation is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organisation shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.’ (PIPEDA, Principle 4.1.3) Comparable does not mean the same, but it does mean generally equivalent.

Consequently, an organisation that transfers personal information to a third party cloud-based service provider for processing remains accountable for the protection of the personal information it transfers. Organisations are responsible for understanding the outsourcer’s personal information handling processes (PIPEDA #2007-377; #2007-386) and must have appropriate confidentiality agreements in place with contractors and provide for same with subcontractors (PIPEDA #2002-42; PIPEDA #2002-35).

Where the information sharing is between a parent company and an affiliate, ‘other means’ of ensuring comparable protections may be adequate in place of a contract, such as a closed private network and a comprehensive strategy and techniques to safeguard personal information (PIPEDA #2006-333).

PIPEDA does not prohibit the transfer of personal information to foreign-based service providers. In assessing whether there exists a ‘comparable level protection’, PIPEDA does not require a side-by-side comparison of foreign laws with Canadian laws, but it does require organisations to be diligent in their dealings with foreign-based providers. For even the best confidentiality agreement cannot override the local laws of a foreign jurisdiction, including laws relating to law enforcement and national security.

According to OPC Guidelines on Processing Personal Data Across Borders (the OPC Guidelines), ‘organisations must take into consideration all of the elements surrounding the transaction. The result may well be that some transfers are unwise because of the uncertain nature of the foreign regime or that in some cases information is so sensitive that it should not be sent to any foreign jurisdiction.’

Safeguards

PIPEDA contains safeguarding obligations that require an organisation to implement reasonable technical, physical and administrative measures in an effort to protect personal information against loss or theft, as well as unauthorised access, disclosure, copying, use or modification (PIPEDA, Principle 4.7). These obligations continue to apply to organisations even when personal information is in the custody of a third party service provider.

OPC guidance provides that organisations must take all reasonable steps to ensure that personal information is safeguarded when in the custody of a third-party service provider. For instance, the organisation must be satisfied that the third party service provider has policies and procedures in place (including training for its staff and effective security measures). The organisation should also have and
exercise, when appropriate, the right to audit and inspect how the third-party service provider handles and stores personal information.

Openness and notice

Although PIPEDA does not require consent of individuals for organisations to transfer personal information to third party service providers, including cloud service providers, for processing directly related to the original purpose for which the personal information was collected, organisations are expected to be open and transparent about this practice – particularly when the transfer occurs across borders. According to OPC Guidelines, ‘organizations need to make it plain to individuals that their information may be processed in a foreign country and that it may be accessible to law enforcement and national security authorities of that jurisdiction. They must do this in clear and understandable language...'(i)deally...at the time the information is collected.’

While provincial private sector privacy laws are generally consistent with the above, there are additional considerations related to transborder data flows that are specific to Quebec and Alberta.

In Quebec, an organisation must take reasonable steps to ensure that personal information transferred to service providers outside Quebec will not be used for other purposes and will not be communicated to third parties without consent (except under certain exceptions prescribed in the Act). The Act also specifically provides that the organisation must refuse to transfer personal information outside Quebec where it does not believe that the information will receive such protection.

In Alberta, organisations that use foreign service providers must include the following information in their policies and procedures:

(1) the countries outside Canada in which the collection, use, disclosure or storage is occurring or may occur; and

(2) the purposes for which the third-party service provider outside Canada has been authorised to collect, use or disclose personal information for or on behalf of the organisation.

Furthermore, in Alberta, notice to individuals must be provided at the time of collection or transfer of the personal information and must specify:

1. The way in which the individual may obtain access to written information about the organisation’s policies and practices with respect to service providers outside Canada; and

2. The name or position name or title of a person who is able to answer on behalf of the organisation the individual’s questions about the collection, use, disclosure or storage of personal information by service providers outside Canada for or on behalf of the organisation.

GTDT: HOW IS THE GOVERNMENT IN YOUR JURISDICTION ADDRESSING SERIOUS CYBERSECURITY THREATS AND CRIMINAL ACTIVITY?

PK: Cognizant of the strategic importance of cybersecurity to Canada’s ‘competitiveness, economic stability and long-term prosperity’, the Canadian government, through Budget 2018, allocated more than C$500 million to support the implementation of the National Cyber Security Strategy (2018) by the government of Canada cybersecurity community, which includes multiple departments coordinated by Public Safety Canada. The 2018 strategy builds on Canada’s first Cyber Security Strategy of 2010 and has
as its main themes:

(1) Ensuring secure and resilient Canadian systems to enhance cybersecurity capabilities and resilience;

(2) Building an innovative and adaptive cyber ecosystem to support advanced research and innovation in the area of cybersecurity; and,

(3) Supporting effective leadership and collaboration between different levels of Canadian government and partners around the world to strengthen the federal government’s leadership role in protecting and promoting cybersecurity in Canada, working in close collaboration with provinces and international allies.

As part of the National Strategy 2018, over C$155 million was specifically earmarked to create a new Canadian Centre for Cyber Security, as part of the Communications Security Establishment (CSE). The aim of the new Centre, announced in June 2018, is to consolidate capacity and expertise, streamline efforts and facilitate coordination across relevant federal departments with operational responsibilities over cybersecurity. It is also intended to provide a unified and outward-facing source of trusted guidance, support and services to Canadians.

Mindful of the increased threats to the country’s national security via attacks on critical infrastructure that spans both public and private sectors, one of the main objectives of the new Centre will be to engage and work more closely with private sector partners in exchanging information about emerging cybersecurity threats and providing advice on means of enhancing cyber resilience.

More specifically, and as per its website:

The Cyber Centre will focus on:

- Informing Canada and Canadians about cyber security matters, as a single, clear, trusted source of information on cyber security for Canadians and businesses
- Protecting Canadians’ cyber security interests through targeted advice, specific guidance, direct hands-on assistance, and strong collaborative partnerships
- Developing and sharing specialized cyber defence technologies and tools resulting in better cybersecurity for all Canadians
- Defending cyber systems, including government systems, by deploying sophisticated cyber defence solutions
- Acting as the operational leader and government spokesperson during cyber security events.

In addition, Bill C-59, described above, would, once passed, strengthen the mandate and authorities of CSE to protect the security and resilience of Canada’s cybersecurity, including a defensive cyber operations mandate to protect Canada and Canadians from foreign cyber threats. Through these and other concerted efforts, the Canadian government has significantly stepped up its efforts to address serious cybersecurity threats and combat cybercrime.

---

**GTDT: WHEN COMPANIES CONTEMPLATE M&A DEALS, HOW SHOULD THEY FACTOR RISKS ARISING FROM PRIVACY AND DATA SECURITY ISSUES INTO THEIR DECISIONS?**

**RSJ:** In contemplating M&A deals, privacy and data security issues are critical considerations during the due diligence stage and eventual determination of whether to proceed with a transaction. As a preliminary matter, Canada’s federal privacy law, PIPEDA, incorporates an express business transaction
exception that allows an organisation that is party to a prospective business transaction to use and disclose personal information without consent when it is necessary to determine whether to proceed with the transaction. In order to rely on this exception, the organisations must have entered into a prescribed confidentiality agreement limiting the disclosure of personal information to only that which is necessary to proceed with the transaction; restricting its use solely for purposes related to the transaction; requiring the recipient organisation to appropriately safeguard the personal information; and, if the transaction is not completed, ensuring the secure return or disposal of such information.

Similar legal requirements apply to permit the ongoing use and disclosure of personal information without consent after the business transaction is completed. Then too, a confidentiality agreement will be required between the parties to the transaction to limit its ongoing use and disclosure solely for purposes for which the personal information was originally permitted to be collected, used or disclosed before the transaction and to ensure its ongoing protection. Individuals must also, within a reasonable time after the transaction is completed, be notified of the transaction and that their personal information has been shared with the ‘new’ organisation, and be given the opportunity to withdraw their consent accordingly.

In determining whether to proceed with a transaction, risks related to privacy and data security and how a potential target organisation has addressed such matters are critical. Parties to a prospective business transaction will want to minimise the risk that they inherit more than they bargained for, as the costs associated with responding to a data-related incident and regulatory investigation are significant. Accordingly, organisations should conduct the necessary due diligence to ensure that the potential target has taken privacy and security risks seriously, and maintains an up-to-date, comprehensive privacy programme. If they do not, it is ‘buyer beware’.

THE INSIDE TRACK

WHEN CHOOSING A LAWYER TO HELP WITH CYBERSECURITY, WHAT ARE THE KEY ATTRIBUTES CLIENTS SHOULD LOOK FOR?

To state the obvious, clients need lawyers who have well-steeped knowledge of, and experience with, Canadian privacy laws across multiple jurisdictions and understand all of the applicable legal requirements from a compliance point of view.

But clients need much more than that. The ideal lawyers to assist an organisation in preparing for, and responding to, cybersecurity incidents are lawyers with lots of ‘mileage’ in this area – lawyers who have assisted many other clients get through some of the country’s largest, most complex, significant and highly publicised data breaches. For example, knowing what questions to ask of the organisation or any vendors involved and what to look for through internal investigations so as to identify the root cause or source of the breach; understand technology well enough to recommend due diligence steps needed or likely to be expected from a legal perspective to curtail the risks of further leakage; when and how to report to regulators, affected individuals and any third parties needed to help mitigate any potential harm; and how to deal with media in crisis management situations to be as transparent as possible from a public relations point of view, while protecting the organisation from liability and preserving solicitor–client privilege as needed. For it is through the past experience of
these many others, that clients can benchmark their own situation and benefit from lessons learned.

Clients also appreciate lawyers with real, practical and hands-on experience dealing with regulators in the context of regulatory investigations and in different scenarios – some of which result in mutually agreeable resolutions, while others are necessarily more challenging – culminating, in some cases, with litigation or potential litigation. Increasingly, lawyers in this space must know what to expect from the regulator’s perspective in terms of investigative processes and best practices. They must be adept at communicating with regulators in collaborative and constructive fashion, but also able to defend their clients’ right to procedural fairness when necessary. Moreover, lawyers must be comfortable dealing with multiple data protection authorities at once and in parallel, given the rising number of joint investigations and the increased level of collaborations between regulators.

Finally, clients should look for lawyers who are able, through their past experiences, to abstract all the critical elements that should form part of a breach incident and readiness response plan. Drawing from lessons learned, lawyers are better able to anticipate the kinds of issues likely to arise - different scenarios and varying modalities – and can thereby help clients plan up front and pre-empt risk accordingly.

WHAT ISSUES IN YOUR JURISDICTION MAKE ADVISING ON PRIVACY AND CYBERSECURITY COMPLEX OR INTERESTING?

The interplay between Canadian privacy laws, anti-spam legislation, consumer protection laws and various other sector-specific requirements makes it challenging, and yet all the more interesting to advise in this area. Likewise, the intersection between privacy law, competition law, and human rights law, adds further layers of complexity and fascination working in this field. As challenging as it may be at times, assisting organisations in navigating these regulatory complexities and achieving practical business solutions can also be incredibly rewarding.

In addition to legal complexities, the era of data analytics and artificial intelligence has raised a whole new dimension of ethical considerations that organisations are currently grappling with and will only intensify from here. The challenge will lie in anticipating, identifying, understanding and addressing ethical issues as part of already well-established PIA and data governance processes. Increasingly, organisations will need to ensure that their innovative data initiatives are not only legally compliant, but also, socially robust, responsible, acceptable and ultimately sustainable. Advising how they might go about doing that in a manner that allows innovation to flourish, while also contextualising it within broader social responsibility will become part and parcel of the privacy lawyer’s critical role. Helping clients define appropriate guardrails as opposed to roadblocks, by developing effective and demonstrable self-governance models will be among some of the most exciting challenges ahead.

HOW IS THE PRIVACY LANDSCAPE CHANGING IN YOUR JURISDICTION?

As in many other jurisdictions, the privacy landscape in Canada is growing more and more complex as a result of rapidly evolving technologies, new and emerging business models, the evolution and maturation of ‘data companies’ and the ever-increasing vulnerability to
cybersecurity threats. Canadian media and the public generally are becoming more demanding in their quest for understanding what is happening to their personal information behind the scenes, pushing back on disrespectful practices and calling for greater transparency of organisations’ and governments’ data management practices.

As a result, parliamentarians have likewise become more engaged on many of the same privacy issues concerning their constituents. Parliamentary committees have recently initiated in-depth studies to examine the privacy implications of Canada’s heightened national security efforts, the privacy of Canadians at the Canada–US border, the advent of connected and autonomous vehicles, the major privacy breach involving Cambridge Analytica, net neutrality and the need for privacy legislative reform in both the public and private sectors. Feeling the ‘competition’ of international regulatory regimes ramping up elsewhere, and seeing Canada’s information laws beginning to pale in comparison, Federal bills have been introduced to revamp Canada’s Access to Information Act, bring amendments to the Personal Information Protection and Electronic Documents Act (PIPEDA) and impose some new privacy obligations on political parties.

Canada has also seen in recent years, and as a result of over a decade of dedicated federal research funding, a significant increase in the capacity of privacy advocacy groups and academic researchers to conduct leading edge studies and publish internationally recognised seminal work in the area of digital privacy. Likewise, the level of sophistication among privacy regulators across the country has significantly increased in recent years, as they leverage capacity and resources through greater collaboration and knowledge exchange between them, and as they seek to innovate in their dual roles of enforcement and promotion.

**WHAT TYPES OF CYBERSECURITY INCIDENTS SHOULD COMPANIES BE PARTICULARLY AWARE OF IN YOUR JURISDICTION?**

Companies in Canada, similar to their global counterparts, face an increasing number of sophisticated cybersecurity incidents. The Canadian Securities Administrators (CSA), an umbrella organisation of Canada’s provincial and territorial securities regulators, conducted a survey of Canadian registered entities in respect of cybersecurity. The survey results are illustrative of the types of cybersecurity incidents experienced by companies in Canada.

Specifically, the CSA survey, released in October 2017, sent to over 1,000 registered firms (of which 63 per cent responded), found that approximately 51 per cent of respondents had experienced a cybersecurity incident during the year surveyed. It identified that the most commonly reported incident was phishing (43 per cent of firms), followed by malware incidents (18 per cent of firms). An additional 15 per cent of survey respondents reported that they had experienced impersonation attempts in order to transfer funds or securities by fraudulent electronic means.
a potential target organisation has addressed such matters are critical. Parties to a prospective business agreement after the transaction is completed, be notified of the transaction and that their personal information will be required between the parties to the transaction to limit its ongoing use and disclosure solely for purposes allowed under applicable local laws.

Similar legal requirements apply to permit the ongoing use and disclosure of personal information to third parties. In particular, parties, along with their lawyers, will need to be sensitive to the use of such personal information to the extent that such use involves obligations that arise under the laws of another country. 

CSE to protect the security and resilience of Canada’s cybersecurity, including a defensive cybersecurity strategy.

In addition, Bill C-59, described above, would, once passed, strengthen the mandate and authorities of the Privacy Commissioner to oversee and enforce the current federal private sector privacy law. This includes the ability to investigate and impose penalties for violations of the act.

(3) Supporting effective leadership and collaboration between different levels of Canadian government

Openness and notice

Organisations are responsible for understanding the outsourcer's personal information handling practices and taking steps to ensure the outsourcer is in compliance with applicable privacy laws.

Under Canada’s federal private sector privacy law (The Personal Information Protection and Electronic Documents Act or “PIPEDA”), organisations are subject to the principles of accountability, safeguards, and openness. These principles require organisations to be accountable for the protection of personal information they collect, use, or disclose, and they must have policies and practices in place to ensure the protection of personal information.

(4) A description of the steps that the organisation has taken to reduce the risk of harm that could result from a breach

The report to the Commissioner shall be sent in writing, by any secure means of communication, and shall include:

(a) The type of personal information involved in the breach

(b) A description of the breach

(c) The identity of the organisation

(d) Contact information that the affected individual can use to obtain further information about the breach

(e) A description of the steps that the organisation has taken to reduce the risk of harm that could result from the breach

(f) A statement that the organisation has notified the Privacy Commissioner

(g) A statement that the organisation will comply with the Commissioner’s directions

(5) A statement that the organisation has notified all other organisations that are in a position to effect any further or corrective action

(6) Contact information that the affected individual can use to obtain further information about the breach

Under PIPEDA, when an organisation determines that there has been a breach of personal information, it must notify the Commissioner as soon as possible. The notification must include the information required by the Act. The organisation must also notify any other organisation that is in a position to effect any further or corrective action. This includes notifying any organisation that may be in a position to prevent the breach from occurring.

(7) A statement that the organisation has notified all other organisations that are in a position to effect any further or corrective action

Organisations shall also notify, as soon as feasible after it determines the breach has occurred, any other organisation that is in a position to effect any further or corrective action. This includes notifying any organisation that may be in a position to prevent the breach from occurring.

Timing

The meline for notifying is short, namely 'as soon as feasible' after the organisation learns of the breach. This means that organisations must act immediately to ensure that any notification is made as soon as possible after the breach is discovered.

For further information please visit www.gettingthedealthrough.com.