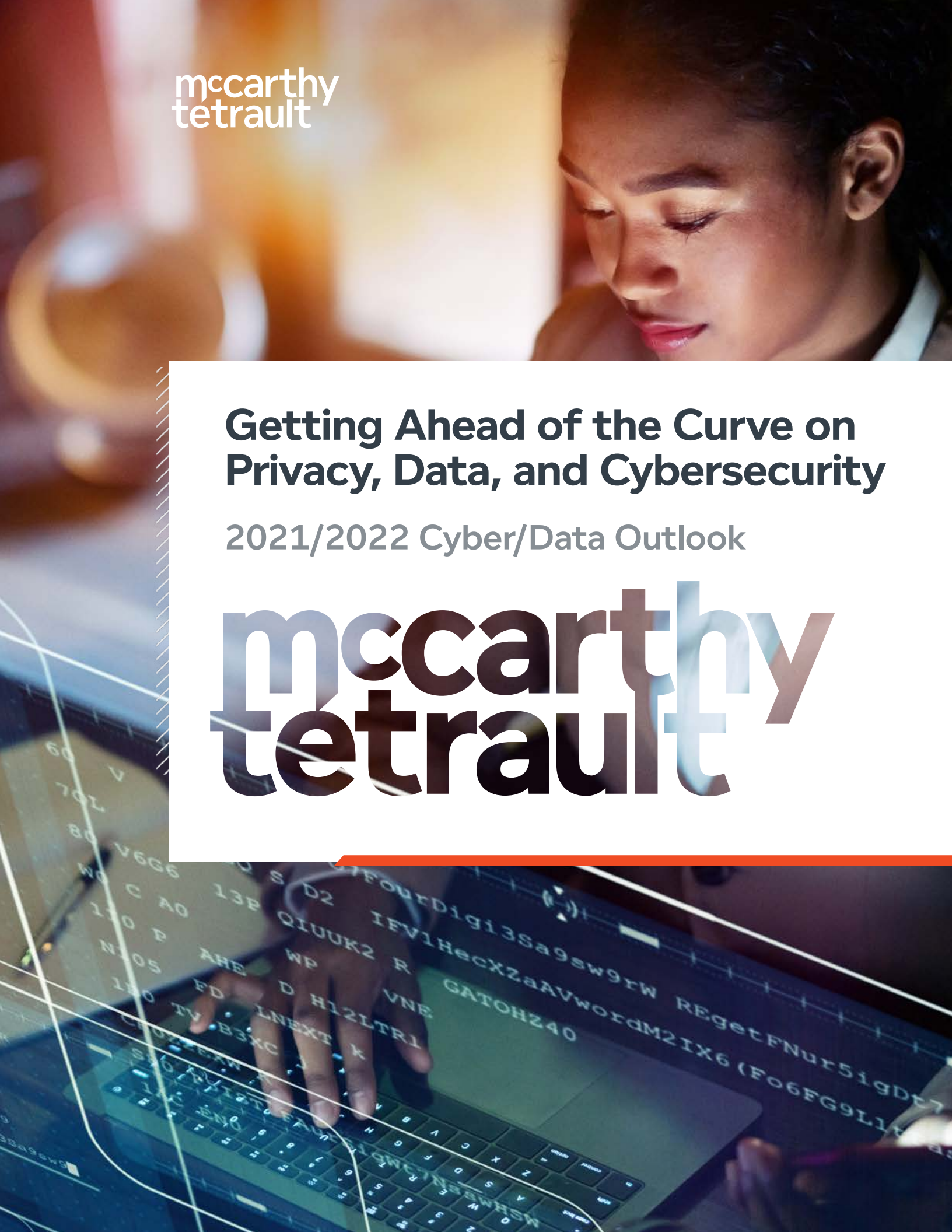


mccarthy tetrault

Getting Ahead of the Curve on Privacy, Data, and Cybersecurity

2021/2022 Cyber/Data Outlook

mccarthy tetrault

Message from our Editors, Marissa Caldwell, Dan Glover, and Charles Morgan:

McCarthy Tétrault's Cyber/Data Group is proud to present the **2021/2022 Cyber/Data Outlook: Getting Ahead of the Curve on Privacy, Data, and Cybersecurity**.

This is the Cyber/Data Group's first Outlook Report. In the Report, our integrated multidisciplinary team highlights key developments in privacy, cybersecurity, and data processing in Canada and globally, and reflects on significance trends and insights for 2022 and beyond. To learn more, please visit our Cyber/Data home page, or speak to one of our talented Authors.

This article is for general information only and is not intended to provide legal advice. For further information, please speak to one of our contacts.

Table of Contents

Introduction

The year 2021 was a watershed year for Canadian privacy, cybersecurity, and data processing. Québec proposed, refined, and passed a landmark new law, and other laws may be on the horizon. The COVID-19 global pandemic continued to change how we live and work, pushing more and more of our lives (and personal information) into the digital environment. Technology continued to advance at a breakneck pace, bringing with it limitless opportunities and complex risks. Competition regulators honed in on the value of data, along with its potential anticompetitive impacts. We saw massive breaches and a vast expansion of ransomware incidents. The courts reasserted their role as gatekeepers in privacy class actions. Insurers took big hits and changed their practices.

In this Outlook Report, our Cyber/Data group takes stock of key developments in Canada and globally during 2021 and reflects on their significance for 2022 and beyond.

Bill 64: A Major Reform of Québec's Privacy Regime

On September 22, 2021, Québec's *Act to Modernize Legislative Provisions respecting the Protection of Personal Information* (Bill 64) received royal assent and became law. Bill 64 provided sweeping changes to Québec's privacy regime, notably by introducing substantial amendments to the *Act Respecting the Protection of Personal Information in the Private Sector* (the Québec Privacy Act). These amendments are set to come into force in three different stages with the first set coming into force on September 22, 2022, and the next set on the same day in 2023, and the final set in 2024.

> **Businesses must obtain an individual's clear, informed, and unambiguous consent for use of their personal information.**

Businesses that retain the personal information of Québec residents are faced with a suite of new obligations and very hefty penalties for non-compliance in the spirit of the European Union's General Data Protection Regulation (the GDRP). Below is a headline summary of the most consequential changes that businesses should be preparing for.

BILL 64: CONSENT AND BASES FOR COLLECTION

Bill 64 provides new consent requirements for businesses that collect personal information. As a baseline requirement, businesses must obtain an individual's clear, informed, and unambiguous consent for use of their personal information.

Where a business obtains consent, it may only use the related personal information for purposes that were originally consented to, with a few exceptions

including if the new purpose is consistent with the original purpose, the new purpose is necessary to detect fraud, or improve security measures, or if the use is necessary to provide or deliver a product or service requested by the individual.

These consent requirements will enter into force on September 22, 2023. Businesses should update their policies and agreements on collection to take into account the above-mentioned factors, and ensure that the appropriate, clarified, and specific consent required for the business' data practices are operationally accounted for.

BILL 64: CHANGES TO RIGHTS REQUESTS FROM INDIVIDUALS

Bill 64 provides individuals a new set of rights which they can assert against businesses holding their personal information. Requests can only be refused with valid reasons. In all cases, whether accepted or refused, businesses must respond to such requests in writing within 30 days. With the exception of the new right of portability (which will take effect on September 22, 2024), these changes are set to enter into force on September 22, 2023.

Right of Portability

Previously, individuals could request access to a copy of the personal information that a business kept about them and have a business confirm the existence of personal information held about them.

Under Bill 64, individuals may now request a copy of the personal information held about them in a structured and commonly used electronic format and that computerized personal information about them be communicated in a commonly used technological format to third parties.

Right to Request De-indexing, Re-indexing or Stopping Dissemination

Individuals can now request that a business cease disseminating information, de-index, or re-index information about them, if the following conditions are met:

- Dissemination of the information causes serious injury to the individual's reputation or privacy;
- The injury is greater than the public's interest, or the interests of free expression; and
- The cessation, dissemination, re-indexation or de-indexation is not greater than what is needed to prevent the injury.

Individuals can now request that a business cease disseminating information, de-index, or re-index information about them.

CORPORATE GOVERNANCE OBLIGATIONS

Bill 64 imposes a series of new obligations relating to corporate governance. The most significant changes are outlined below.

Person in Charge of Personal Information

Businesses must appoint a "Person in Charge of Personal Information" (the PCPI) to oversee and serve as the primary contact point for the business' treatment of personal information. By default, the person with the highest authority within the organization inherits the role of PCPI. This responsibility can, however, be delegated in writing to any other person, including a person external to the business. The PCPI's contact information and position must be published on the business' website. The PCPI is

also responsible for answering any rights-based requests made by individuals.

In addition, the PCPI must provide input on any project involving the acquisition, implementation, or redesign of a system involving personal information. When a privacy impact assessment is conducted, the PCPI is to provide input on privacy issues. The obligations relating to the PCPI will come into force on September 22, 2022, which make this a high-priority item for any business collecting personal information.

Disclosure of Privacy Policies and Governance Procedures

Businesses must now maintain internal governance policies and practices and publish information about them in simple and clear language. These policies must contain baseline information on the following aspects of the business' practices concerning personal information:

- The framework for keeping and destroying personal information;
- Roles and responsibilities for personnel throughout the life cycle of personal information; and
- Process for dealing with complaints.

Businesses must also make public their confidentiality policies (commonly referred to as "privacy policies") and ensure they are drafted in simple and clear language, including any subsequent amendments.

Incident Registration and Breach Notification Requirements

Businesses will be required to record any confidentiality incident in an internal incident registry, and provide the incident registry to the Commission d'accès à l'information (the CAI) upon request. When recording confidentiality incidents, the means used to resolve or remedy the vulnerability must be a part of the internal incident report. In addition, any member of a business that has reason to believe a confidentiality incident has occurred must take reasonable measures to reduce the risk to the personal information of individuals.

Where an incident presents a "serious risk of injury," businesses must promptly notify the CAI, and any person whose personal information is affected by the incident, unless it would hamper an investigation into the incident. Breach registry requirements are set to come into force on September 22, 2022, making them a high-priority item for compliance. Note that similar obligations already exist under the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and Alberta's *Personal Information and Protection of Privacy Act*.

Where an incident presents a "serious risk of injury", businesses must promptly notify the CAI, and any person whose personal information is affected by the incident

Privacy Impact Assessment

Bill 64 adds the obligation for businesses to conduct privacy impact assessments prior to the transfer of personal information outside of Québec. In addition to the requirement to obtain consent or codify a contract in writing detailing the transfer information to third parties

prior to collection, the privacy impact assessment must determine that the personal information would receive "adequate protection" in the target transfer jurisdiction.

Businesses will also be required to conduct privacy impact assessments for any project to acquire, develop, or overhaul an information system or electronic service delivery system involving the collection, use, communication, keeping or destruction of personal information. This will likely impact the contracting for many technology tools or storage solutions used by most businesses.

Privacy impact assessments must specifically take into account the following factors:

- The sensitivity of the information;
- The purposes for which the information is to be used;
- The protection measures, including those that are contractual, that would apply; and
- The legal framework applicable in the jurisdiction to which the personal information is being communicated.

The privacy impact assessment must be proportionate to the sensitivity of the information being assessed. In addition, transfers to third parties must be subject to a written agreement that mitigates the risks identified in the privacy impact assessment.

The requirements for third party transfers come into force on September 22nd, 2023, giving businesses more time to prepare.

INCREASED PENALTIES

One of Bill 64's most significant changes is the potential for significant penalties for failing to comply with the Québec Privacy Act's provisions. Potential administrative and penal fines mirror, and in some cases, exceed the hefty fines under the GDPR.

The CAI can impose administrative monetary penalties for failures to adhere to the Québec Privacy Act's provisions. Companies that contravene these provisions may enter into an undertaking with the CAI to remedy the default, and avoid an administrative monetary penalty. Otherwise, the CAI can impose a maximum penalty of C$10,000,000 or 2% of worldwide turnover for the preceding fiscal year, whichever is greater.

The CAI can impose administrative monetary penalties for failures to adhere to the Québec Privacy Act's provisions to a maximum penalty of C$10,000,000 or 2% of worldwide turnover for the preceding fiscal year.

In the event of a failure to report confidentiality incidents, refusal to comply with an undertaking from the CAI, or the use, collection, or communication of personal information in contravention of the Québec Privacy Act, the CAI may instead institute penal proceedings in court with a potential maximum penalty of C$25,000,000 or 4% of worldwide turnover for the preceding fiscal year, whichever is greater.

In the case of repeated failures to adhere to the Act's provisions, the above-listed penalties can also be doubled for subsequent violations.

Anticipated Changes to Privacy Laws in Canada

Privacy compliance was once a straightforward process of checking the right boxes — not much more than adequate consents and a privacy policy on a website — but that world no longer exists. We are in the midst of a global explosion of legislation governing data. With potential overlaps and even clashes between laws, as data flows grow more complex, organizations are now forced to navigate privacy legislation from multiple jurisdictions, different levels of government, and even industry-specific regulations and guidance, with increasingly harsh penalties for non-compliance.

Keeping up with what's happening in this changing environment will help you avoid the quicksand without relinquishing the legitimate business purposes for using data. The following pages summarize anticipated changes relating to privacy legislation, cross-border data transfers, and sensitive data requirements such as biometric data and automated decisions.

WHAT'S ON THE TABLE IN CANADA?

Québec: Passed in September 2021, Québec's Bill 64 is set to shake the Canadian privacy landscape with a fundamentally new GDPR-inspired law with massive penalties for non-compliance of up to 8% of annual worldwide turnover for repeat offenders. Bill 64 introduced unique cyber incident reporting obligations, including a requirement to notify individuals if a confidentiality incident poses a "risk of serious injury," as well as to take reasonable measures to reduce the risk or injury and prevent new incidents. The new transparency and consent standards require that consent be clear, free, informed and provided for specific purposes, which is a higher standard than that imposed by Canada's current federal privacy legislation, PIPEDA. The operational requirements for cross-border transfers of personal information of Bill 64 task organizations with conducting impact assessments using prescribed privacy-related factors prior to communicating personal information outside of Québec. Privacy by default and privacy by design provisions will require a real change in mindset when acquiring technologies and designing new programs. New user rights will require new compliance approaches. Bill 64 starts to come into force in September 2022, with the penalties and most of the key provisions coming into force in September 2023.

Federal: Proposed in 2020 and potentially back on the table in similar form within the coming year, Bill C-11 would repeal PIPEDA and enact in its place the *Consumer Privacy Protection Act* (CPPA) and the *Personal Information and Data Protection Tribunal Act* (PIDPTA). The CPPA seeks to introduce new requirements for data protection in Canada and would apply to personal information that is collected in Canada. Although the Privacy Commissioner of Canada has referred to the legislation as a "step backwards," if reintroduced and passed in similar form, Bill C-11

would significantly alter the Canadian privacy landscape, as it would pair important requirements with significant penalties of up to 5% of an organization's gross global revenues.

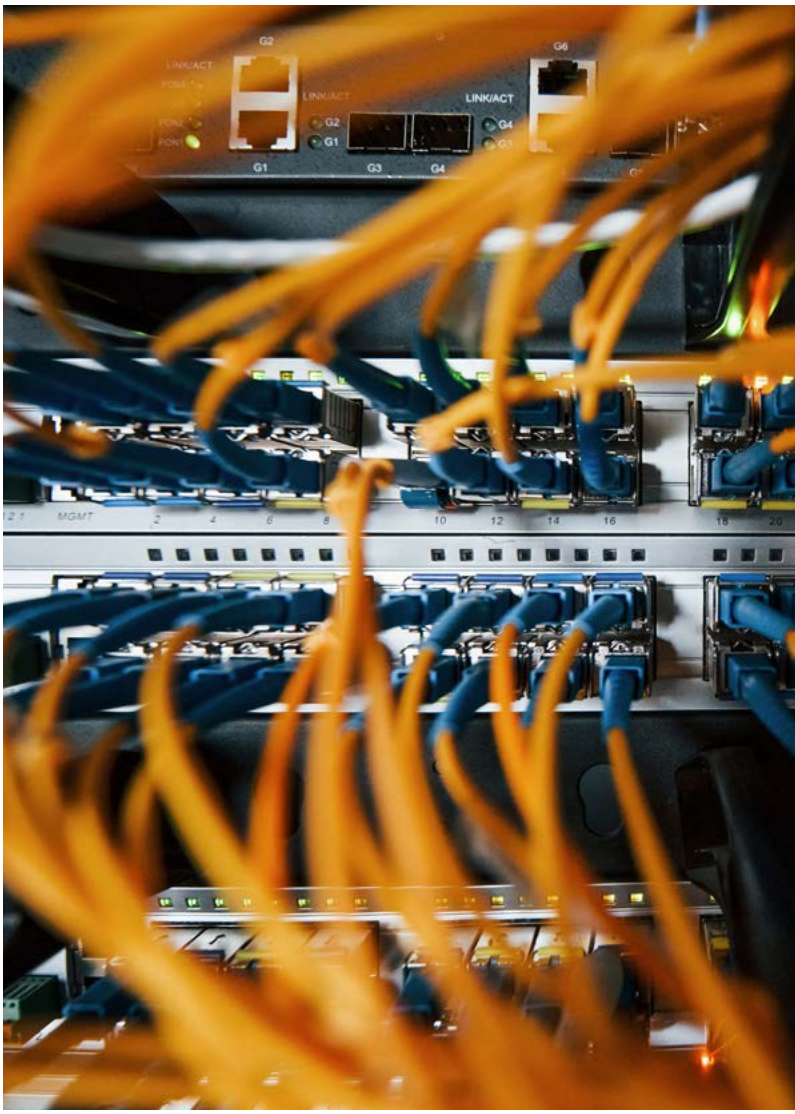
Ontario: Released in June 2021, the white paper *Modernizing Privacy in Ontario* proposes substantial changes for a new provincial privacy statute. Broadly speaking, the white paper proposals suggest implementing stricter and less flexible requirements than those proposed in the CPPA. Although rumoured to be on the back burner as the provincial government focuses on other priorities, if introduced and passed, the *Modernizing Privacy in Ontario* model would introduce GDPR-inspired rights, enforcement, and penalties, including for employee personal information that currently falls into a grey area for most Ontario businesses. Also worth perusing is the Ontario IPC's response to *Modernizing Privacy in Ontario*, which sets out an extensive wish list, including empowering the IPC to offer compliance support tools, such as advisory services, sectoral codes of practice and certification programs, with a special focus on "agile" regulation of SMEs. Helpfully, the IPC also calls for penalty powers that include "consideration of any regulatory action already taken by other jurisdictions as a possible mitigating factor, ensuring a harmonized, fair and proportionate approach."

The Ontario IPC also calls for penalty powers that include "consideration of any regulatory action already taken by other jurisdictions."

British Columbia: This fall, Bill 22 was introduced and passed in British Columbia to amend the *Freedom of Information and Protection of Privacy Act* (FIPPA). A notable change that would affect public bodies in the province is the elimination of the requirement for storing and allowing access to personal information only from within Canada. This would increase the number of service providers the government could access, as many providers do not have a physical presence in Canada. Bill 22 makes room for the possibility that these cross-border data transfers would be governed by regulations and permitted.

CURRENT TRENDS

Classifying the Nature of Privacy Rights: Not only are we seeing specific rights — such as the right to be forgotten or the right to data portability — explicitly enumerated within privacy legislation, but there are some murmurs that proposed laws could recognize privacy as a fundamental right. For example, in modernizing its privacy legislation, the Ontario white paper is considering the possibility of recognizing a fundamental right to privacy within the preamble of the provincial privacy legislation. Currently, Québec is the only province that recognizes



a right to privacy, which is explicitly set out in s. 5 of the Québec *Charter of Human Rights and Freedoms and Civil Code*. The OPC has criticized the lack of a rights-focused preamble and purpose clause in other proposed legislation, including the CPPA, but has not yet seen its lobbying efforts bear fruit federally.

This consideration arises at an interesting time, namely one in which the courts seem to be questioning the value of describing privacy as a "quasi-constitutional right."

In 2021, the Supreme Court of Canada characterized "the nature of limits of privacy as being in a state of 'theoretical disarray'" and cautioned that "recognizing an important interest in privacy *generally* could prove to be too open-ended and difficult to apply." It emphasized that "much turns on the context in which privacy is invoked." These statements followed other Supreme Court decisions of the past decade (*Royal Bank of Canada v. Trang, Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers*), in which privacy rights gave way to more compelling competing interests, demonstrating that contextual evaluations of privacy is the preferred judicial approach. Given the broad spectrum of privacy protections — spanning from a name and mailing address to the most intimate and impactful information about a person — as well as the propensity for privacy to clash with fundamental rights and values, the reluctance to treat privacy as a unitary concept seems a wise approach.

Much Higher Penalties: Currently, PIPEDA only permits maximum fines of C$100,000 for indictable offences. Bill C-11 would see that tribunals could impose fines of up to C$10 million or 4% of an organization's gross global revenue, and that more serious offences could lead to fines of the higher of C$25 million or 5% of gross global revenue.

Bill C-11 would see that tribunals could impose fines of up to C$10 million or 4% of an organization's gross global revenue.

In Québec, Bill 64's penalty clauses are even more severe, with repeat offenders exposed to penalties of C$50 million or 8% of annual worldwide revenues, whichever is greater. Unhelpfully, the legislative penalty factors do not take into account the potential for penalties being awarded elsewhere premised on the same facts, thus potentially leading to "multiple jeopardy" for a privacy incident that crosses many borders and attracts the attention of many regulators.

Separation of Investigation and Decision-Making Powers: If reintroduced and passed in similar form, the CPPA would grant enhanced oversight authority to the Privacy Commissioner of Canada through a range of auditing, investigating, and order-making powers. The greatest departure from existing privacy law regimes both at home and abroad would be the creation of a tribunal that would hear administrative appeals following decisions rendered by the Privacy Commissioner of Canada. The tribunal would also be able to impose financial penalties. The tribunal would provide a layer of independence compared to existing structures in Canada, where there is a concern that the "judge, jury and executioner" are all working out of the same regulatory agency. The complexities of this regime is discussed at more length in our blog on The CPPA's Privacy Law Enforcement Regime. By contrast, the CAI in Québec is taking carriage of enforcement matters under Bill 64, with fining powers of 2% of annual worldwide turnover or C$10 million. It has promised to develop and make public a general framework for the application of administrative monetary penalties before Bill 64 comes into force.

CROSS-BORDER DATA TRANSFER COMPLEXITIES

Canada's Adequacy Decision: Under a 2001 decision by the European Commission (most recently reaffirmed in May 2018), Canada is considered as providing an adequate level of protection for personal data transferred from the EU to recipients subject to PIPEDA, while in 2014, the EU Article 29 Working Party did not recommend that Québec receive a favourable adequacy assessment until certain improvements were made to its private sector law. Article 45(4) of the

GDPR requires the Commission, on an ongoing basis, to monitor privacy-related developments in Canada that could affect the functioning of the existing adequacy decision. Unless Canada amends its federal data protection laws prior to the next review (which occurs every four years, beginning in May 2020), it is widely expected that Canada would not maintain its current adequacy status. Where there is no adequacy decision, a Transfer Impact Assessment must be completed (see full recommendations in PDF form).

Divergent Approaches: The cross-border data transfer requirements of Bill 64 are a sharp contrast to the CPPA's liberal approach that would not restrict the transfer of personal information outside of Canada or require organizations to undertake impact assessments for such transfers. Under Bill 64, before communicating personal information outside of Québec, an organization must conduct a Privacy Impact Assessment (PIA) and then enter into a written agreement that considers the outcome of the PIA and establishes adequate protections taking into account the sensitivity of the personal information, the purpose for which it is to be used, safeguards, and the receiving jurisdiction's legal framework.

TRENDS IN BIOMETRICS & AUTOMATED DECISION MAKING

Automated Decision Making: Following Bill 64, Québec is the first Canadian jurisdiction to introduce a right to be informed about decisions made with automated decision systems (ADS). Being informed about an ADS decision includes being informed about the principal factors and parameters that resulted in the decision, as well as the ability to comment or object to the decision. This means that companies need to get prepared to explain the ADS. The CPPA proposed similar ADS requirements, including requiring organizations to publish a general account of their use of any automated decision system to make predictions, recommendations or decisions about individuals that could have significant impacts on them, as well as an explanation of a prediction, recommendation or decision made about a specific person.

Québec is the first Canadian jurisdiction to introduce a right to be informed about decisions made with automated decision systems (ADS).

Ontario's white paper proposal goes one step further, prohibiting ADS where the decision would significantly affect an individual, unless the individual's express consent is obtained, or such a decision is authorized by law or necessary under contract. This is consistent with Article 22 of the GDPR, which (subject to certain exceptions) provides that data subjects shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects. It also prohibits decisions based on the "special categories" of data, including race, political opinions and biometric data for the purpose of uniquely identifying a natural person. Automated decisions are permitted if the decision is necessary for entering into or the performance of a contract, authorized by the Union or Member State law, or based on the data subject's explicit consent.

How to Prepare: Organizations that currently use or plan to use AI systems for their activities should prioritize two items:

(i) an Algorithmic Impact Assessment to identify the level of impact the ADS may have and to assess the possible harms;
(ii) conveying the ADS in a manner that ensures consent; and
(iii) providing a mechanism for human review of ADS.

In Canada, Algorithmic Impact Assessments requirements have only been seen in the *Directive on Automated Decision-Making*. Although it is limited in scope and only applicable to the public sector, the Directive is consistent with the increasing demand for impact assessments in a variety of contexts.

Biometrics: In keeping with the greater enforcement powers cropping up in privacy legislation, Québec's *Act to Establish a Legal Framework for Information Technology* (AELFIT) provides for a new 60-day deadline to disclose to the CAI the creation of a biometric feature or measure bank before it is deployed. Express consent before the use of biometrics is required.

How to Prepare: These two features — oversight and consent — are in keeping with the principles-based approach applied in Canada and will likely continue into the future. If your organization is considering using biometric data, be sure to crystallize a plan using the life cycle of the data as a guide.

STRATEGIES FOR SUCCESS

Privacy legislation is top of mind for legislatures across the world. Organizations need to be prepared to adapt to new privacy legislation from various levels of government within the narrow time frames prescribed by law, or risk facing hefty fines for non-compliance.

Impact Assessments: Whether Privacy, Transfer, or Algorithmic, the trend toward mandating impact assessments across increasingly diverse contexts is likely to continue. Although PIPEDA imposes no such requirement, Bill 64 introduced impact assessments when transferring data outside of Québec and acquiring, developing or overhauling an information or electronic service delivery system involving the handling of personal information. The CPPA would introduce a variation on the theme by requiring a privacy management program be implemented. The GDPR already mandates impact assessments when there is a high risk to the rights and freedoms of natural persons, such as when new technologies or ADS are used.

How to Prepare: Ensure that your organization has organization-specific impact assessment templates, in addition to internal standard operating procedures (SOPs) that flag when to conduct mandatory and recommended impact assessments based on legislative requirements. Recognize that different jurisdictions have different requirements for when and how to conduct impact assessments.

Anonymization and Minimization: Under PIPEDA and the GDPR, de-identified information is not "personal information" because it is not information about an identifiable individual. Although there is some ambiguity in the CPPA, the proposed "de-identification" changes appear to treat all de-identified information as being subject to the CPPA. This could jeopardize the harmonization of our laws within Canada and potentially damage our countries' ability to compete. For more information, please see our article: CPPA: Identifying the Inscrutable Meaning and Policy Behind the De-Identifying Provisions.

How to Prepare: Innovative approaches to the anonymization of data, such as suppressing, scrambling and generalizing data, can reduce the need for storing personal information while maintaining the quality of analytics. For a more detailed analysis, please read the below section on Strategic Uses of Data Anonymization and Data Minimization in Data Analytics.

Know your Data: Identifying and locating personal information, and then automating this process, will be the key to ensuring compliance with current and future laws.

How to Prepare: Knowing your data requires implementing an information governance strategy to identify personal information, developing clear policies and procedures to manage the lifecycle of the data, creating a data map to track where the information is stored, leveraging technology to help implement the policies, and training employees to manage personal information.

Cyber/Data Considerations in the Workplace

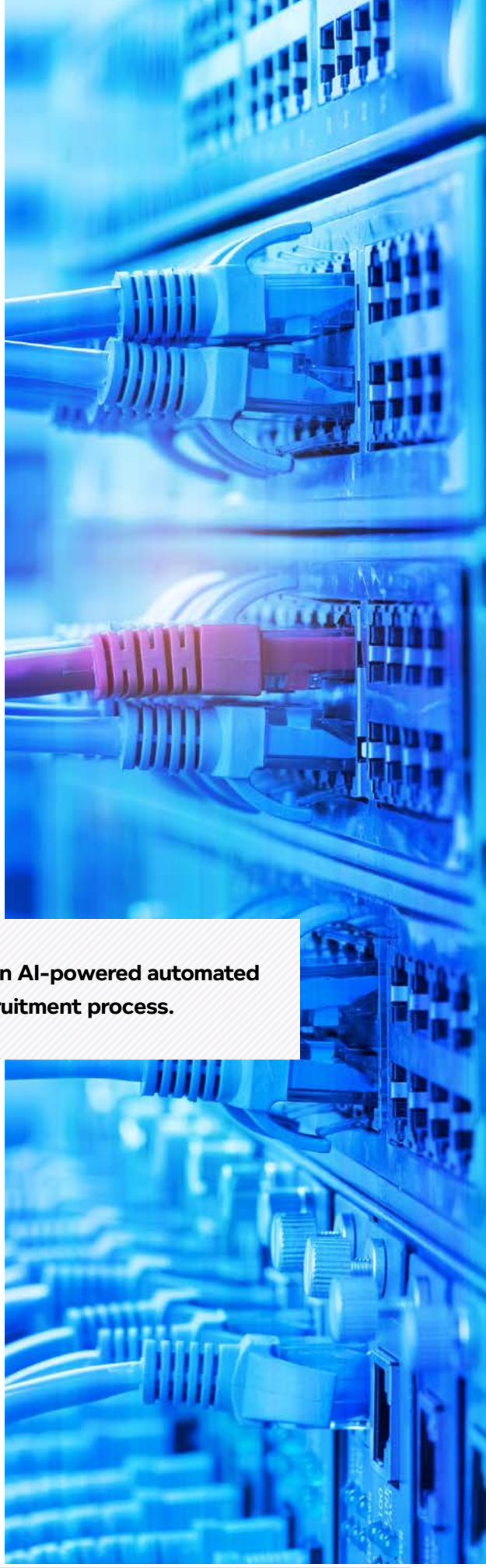
The Ethics of Using Artificial Intelligence in Recruitment and Talent Management

The adoption of artificial intelligence (AI) by employers and recruitment agencies has ethical implications that must be managed.

AI is the science of improving the intelligence of machines, often for the purpose of automating tasks or streamlining decision-making. Many large employers and recruitment agencies may use or rely on AI-powered automated applicant tracking systems (ATS) to screen candidates in the recruitment process. Some may rely on AI tools for candidate testing and/or for evaluating candidate interview responses.

Beyond recruitment, employers are also turning to the use of AI to conduct employee sentiment analysis for the purpose of talent management. Survey results and emails from employees are analyzed to evaluate tone and mood, thereby determining how employees feel about the organization and their role within it.

Overall, managing an employer's reputation and mitigating legal risks requires considering not only the opportunities but also the potential pitfalls with using AI in the aforementioned ways.



Many large employers and recruitment agencies may use or rely on AI-powered automated applicant tracking systems (ATS) to screen candidates in the recruitment process.

POTENTIAL LEGAL RISKS ASSOCIATED WITH THE USE OF AI

The outcomes produced by AI analysis tools are often only as reliable as the data and parameters with which they were designed and trained. Moreover, in some cases, the use of such systems has served to reinforce bias that existed in the data sets upon which the AI systems are trained.

All Canadian jurisdictions have human rights legislation which protects individuals from discrimination in employment on the basis of enumerated prohibited grounds, also often referred to as "protected characteristics." These protections under human rights legislation extend to recruitment processes. The listed enumerated grounds may vary slightly by jurisdiction, but typically will include, *inter alia*, race, origin, creed, sex, family status and disability (physical or mental).

Some Canadian jurisdictions also have accessibility legislation containing

requirements for the accommodation of individuals with disabilities in recruitment processes and in employment. For example, Part III Employment Standards of the Integrated Standards Regulation made under the *Accessibility for Ontarians with Disabilities Act* sets out specific requirements for recruitment, including offering candidates with accommodation in assessment or selection processes. It also contains the requirement that an employer will take into account the accessibility needs of employees with disabilities in performance management processes.

A 2018 report for the Council of Europe noted that every stage of the design process presents a risk that AI will adopt a discriminatory approach to data analysis. Bias can enter the AI analysis despite the best intentions of the designer. This can occur even when protected characteristics data is not collected due to the existence of 'proxies,' which are other collected data points that correlate with protected characteristics. For example, there are documented instances of racial bias in AI applications used for the purposes of facial recognition, criminal sentencing, health-care risk assessment and loan eligibility assessment.

The risk of bias in AI analysis extends to tools used for recruitment and talent management. Defining what characteristics of a "good" employee requires prioritizing certain characteristics over others in the design of the AI analysis. This can result in bias entering the AI analysis, which may be compounded when the AI tool makes use of data from the internet in evaluating candidates or employees. The selection of characteristics and the process of measuring them could potentially result in an unfair disadvantage for people with disabilities. For example, many candidates with disabilities struggle with one-way video-interviewing where AI is used to evaluate answers to questions.

EMPLOYER BEST PRACTICES FOR THE USE OF AI

Employers can implement policies and practices to limit the risk of biased decision-making when using AI tools. Human oversight of AI analysis can filter out bias when a person is tasked with evaluating AI output and making final decisions. Furthermore, when procuring AI software, employers should consider conducting AI ethics impact assessments. AI ethics impact assessments will evaluate the accountability, fairness, transparency, explainability, accuracy and reliability of AI tools and their outputs. An internal committee could then evaluate the results of these assessments and address concerns before making a purchasing decision.

Employers can play a significant role in ensuring that AI is fair by incentivizing developers to design responsible AI. Employers who are regular clients of AI software developers can voice their ethical concerns and request the requisite information to assess the ethics of the software. In addition, employers can push for the prioritization of diversity in employment practices at AI firms. Part of the source of bias in AI tools can be the lack of diversity on developer teams.

Employers should implement data storage and processing practices that protect the privacy of data subjects from whom data is collected. Many enterprises keep Records of Processing Activities (ROPAs) that track key metrics for every data collection and processing activity undertaken, including by AI software. With respect to each processing activity, ROPAs track: the controllers and processors of data, the purposes for processing, the categories of data subjects, personal data, and recipients of data involved, retention schedules for data, and security measures in place. ROPAs create a data processing crumb trail, which can be reviewed for internal purposes as well as utilized for the purposes of managing risks and mitigating against potential liability.

Employers can play a significant role in ensuring that AI is fair by incentivizing developers to design responsible AI.

Employers have many options at their disposal for addressing the risks of using AI. AI technologies are expected to be adopted in virtually every industry in the future. Employers who are ahead of the curve with AI risk management will optimize their talent recruitment and performance management processes while protecting their reputation and managing their potential liability.

Privacy Considerations During Workplace Investigations

In recent years, legal requirements to conduct workplace investigations, including, for example, where there are allegations of workplace violence or harassment under the *Occupational Health and Safety Act*, have resulted in an increase in the number of workplace investigations. Workplace investigations also often take place to address misconduct, whistleblower complaints, as well as complaints of discrimination. A consideration which needs to be addressed in a workplace investigation procedure is confidentiality, privacy and the protection of the information gathered in the course of the investigation. These considerations have become more pressing given that many investigations are being conducted virtually or by teleconference calls due to the COVID-19 pandemic.

APPROPRIATE MEASURES MUST BE IN PLACE TO PROTECT INFORMATION

The first step to a workplace investigation is appointing an appropriate investigator. An investigator, whether they are internal or external to the company, must have in place appropriate measures to ensure the confidentiality and protection of the information that they receive in the course of the investigation. In general, a best practice approach is to maintain confidentiality over the information in an investigation except to the extent that disclosure is required by law or is necessary for the purposes of the investigation on a "need to know" basis. To the extent that an applicable workplace policy contains requirements for confidentiality, protection, storage and retention of information, the investigator must comply with the policy.

> **An investigator must have in place appropriate measures to ensure the confidentiality and protection of the information.**

This means ensuring that electronic and physical copies of emails, documents or folders relating to the investigation cannot be viewed by others. Physical materials should be stored in a manner that cannot be accessed by others and electronic materials should be password-protected. The recipients of any information about the investigation or its conclusions should be carefully considered in order to control the circulation of information. If an investigator is reviewing documents or drafting a report in a co-working space, the investigator should take measures to ensure that their screen cannot be viewed.

When the investigator first meets with any individual they are interviewing in the course of an investigation, the investigator should inform the individual of the confidentiality required for the investigation, the potential consequences for failing to maintain confidentiality, and

confirm for them the purposes for which the information they provide to the investigator will be used. An investigator should avoid making promises to any individual regarding confidentiality, in case information needs to be disclosed in the course of the investigation or to the employer in order for corrective actions to be taken.

EMPLOYEE MONITORING

The investigator should be aware of any privacy law implications that may arise during the investigation. Special attention should be given where the investigation involves employee monitoring and surveillance. Generally, the employer may conduct employee monitoring if the monitoring is reasonable regarding both (i) the purpose that the employer conducts the monitoring and (ii) the manner that the employer carries out the monitoring. The employer must generally provide advance notice of monitoring to employees and, in some provinces, must obtain consent from the employees. It is reasonable in most cases for an employer to place a notice in a spot likely to come to the attention of individuals who will be on camera letting them know that there is video surveillance or monitoring taking place.

Advance notice is not generally required if either the monitoring is reasonable for the purposes of investigating a breach of the express or implied terms of employment, or the employer has a reasonable basis to believe that a breach has or will occur.

CUSTODIAN DEVICES

Custodian devices are electronic devices that the employee has custody of, but are owned by the employer (for example, a mobile phone or laptop). The reasonable expectation of privacy and other rights that the individual has in devices owned by the employer are likely much lower and less significant than the rights the employee would have in a device that the employee personally owns.

An employer can diminish an employee's expectation of privacy in these devices by requiring the employee to sign off on and/or be trained in a policy that sets out and reserves the right of the employer to monitor the device(s) and to have access to and ownership over its contents. Employers are generally not prohibited from accessing communications that are stored on their own electronic network (for example, employer's email server) if the access is authorized under the employer's own policies. Where the police are conducting a criminal investigation at

the workplace, evidence may be excluded from trial if there is not a valid warrant (*R. v. Cole*).

IMPROPER EVIDENCE COLLECTION MAY IMPACT INVESTIGATION

An employer may be prevented from relying on the findings of its investigation to justify corrective action (such as a suspension or termination for cause, for example), if evidence is collected in an improper manner.

When investigating a non-unionized employee, improper employee monitoring or gathering of evidence can lead to a number of deleterious outcomes such as: damages under statutory torts of privacy; damages under the common law tort of privacy; and claims for constructive dismissal, moral damages and punitive damages (*Colwell v. Cornerstone Properties Inc.*).

When investigating a unionized employee, where there is an absence of a specific collective agreement provision addressing employee monitoring, an arbitrator will typically assess whether the evidence gathered through monitoring is admissible. If an arbitrator determines that the employee was improperly monitored, the arbitrator can order the exclusion of such evidence. An arbitrator will balance the employee's right to privacy with the employer's right to investigate to determine if the evidence is admissible. In making this determination, arbitrators generally consider whether the monitoring was reasonably required in light of the circumstances, whether the employer conducted the monitoring in a reasonable manner, and whether there were alternatives to the monitoring (*Doman Forest Products Ltd. v. I.W.A.*).

There are many considerations that must be taken into account in the course of a workplace investigation. The requirements governing the collection, use and storage of information during investigations are a key part of any investigative procedure and play a significant role in ensuring the employer's compliance with applicable privacy law and the integrity of the investigation outcome.

Strategic Uses of Data Anonymization and Data Minimization in Data Analytics

Data analytics is undergoing a watershed moment internationally that is likely to impact common industry norms. In Québec, of course, Bill 64 and its draconian penalties will come into force largely in September 2023, including Canada's first statutory treatment of technologies "that allow a person to be identified, located or profiled." Europe is even farther ahead: on November 23, 2021, the Internal Market and Consumer Protection Committee of the European Parliament unanimously backed the proposed *Digital Markets Act* (the DMA), which sets to prohibit the use of combined personal information to deliver targeted advertising by major advertising platforms.

Providers of data for targeted advertising and data insights have also felt pressure from lawmakers regarding third-party tracking, which often takes the form of third-party cookies inserted into browsers that track users to gather information on their behavioural patterns and interests. The industry is in the midst of a significant upheaval: Firefox and Safari have blocked third-party cookies from their browsers entirely, Apple has implemented privacy settings to their mobile devices through iOS 14.5 to require opt-in to third-party tracking on apps, and Google has committed to phasing out its third-party cookie system by 2023.

Data analytics is a constant battle between the utility and the anonymity of the underlying data set. Businesses may wish to anonymize personal information to simplify regulatory obligations and reduce breach risks, while retaining enough critical personal information for the data to be useful. This leads to a pivotal question — how can businesses learn the most about group behaviours while knowing as little as possible about the specific individuals in the group?

> **Businesses may wish to anonymize personal information to simplify regulatory obligations and reduce breach risks, while retaining enough critical personal information for the data to be useful.**

Facing increased regulatory scrutiny, businesses have come up with unique solutions to retain critical personal information, while minimizing privacy risks associated through anonymization. By strategically applying anonymization techniques, businesses maximize the analytical value of personal information, while minimizing the risks associated with keeping personal information. In doing so, the risk of harm associated with privacy violations, regulatory investigations, and disclosure obligations can be reduced as personal information held by a business ceases to specifically identify individuals, or greatly reduces potential harms to those individuals. We discuss these solutions below.

COMMON ANONYMIZATION AND MINIMIZATION TECHNIQUES

Privacy regulators have increasingly supported the use of anonymization techniques to reduce the risks associated with businesses processing and keeping personal information. As a useful guideline, the European Commission identified three factors to assess the level of security provided by an anonymization technique: (i) is it still possible to single out an individual?; (ii) is it still possible to link records relating to an individual?; and (iii) can information still be inferred concerning an individual?

In practice, perfect anonymization of data would render data nearly unusable from a business perspective. However, businesses can implement a variety of anonymization and minimization techniques that preserve the analytical usefulness of data to draw business insights, while at the same time protecting personal information from being widely disseminated. As these techniques technically permit the re-identification of data for analysis purposes, they are referred to as "pseudo-anonymization." Through a combination of methods for pseudo-anonymizing personal information, businesses have implemented a variety of creative ways to maximize analytical usefulness while reducing the legal risk involved with data processing.

Suppression

Data suppression is the practice of eliminating certain categories of data that are irrelevant to a given analytics exercise. As an example, if the full name of an individual is irrelevant to analytics but was collected as part of the payment information process, the full name would be removed from any analyst's request for data. Ideally, suppression should be used when a category of personal information is either irrelevant or when the category cannot otherwise be suitably anonymized with another technique, as the data cannot subsequently be recovered.

Masking

Masking is similar in principle to suppression, but a less permanent method of anonymizing data. The technique involves replacing characters in personal information with dummy characters to reduce the possibility of unauthorized access to sensitive data. A common example is the use of uniform characters when inputting a password to prevent recording (i.e. passwords become • • • • • • • • when typed). The same practice is used to mask credit card information, replacing numbers with XXXX-XXXX-XXX-1234 to prevent malicious use. Masking can be a useful, but non-permanent, means of providing added security by preventing the widespread dissemination of sensitive personal information across an organization.

Mixing, Scrambling or Shuffling

This process describes either shifting the letters or digits of personal information within one instance of personal information, or across an entire data set. By dissociating the logical order a data set comes in, the amount of identifying information that can be extracted by malicious actors is significantly reduced. In addition, information that goes through a scramble or mixing makes the process of identifying the personal information of other data subjects by attempting to decode the mixing process more complicated, as the columns or data set subject to a mixing process is most often randomized on each access instance.[1]

Generalization

Generalization involves deliberately reducing the accuracy of a data set to comprise a range or broader definition. Data categories that benefit from generalization are often those whose analytical value is preserved even when abstracted to a certain degree. For service offerings, an example can include moving from a specific postal code to the first three digits of that code or even to a broader neighbourhood

1. For a concrete example of shuffling, see Imperva, What Is Data Anonymization."

level. Another example would be to move from a specific data of birth to month/year of birth to a specific age (55) to a general age range (50 to 60). Generalization is most effective when implemented selectively, as how much a data value is generalized has a strong impact on the protection afforded to individuals in the data set.

Generalization is most effective when implemented selectively, as how much a data value is generalized has a strong impact on the protection afforded to individuals in the data set.

Adding Noise

The process of adding noise hides personal information collected by adding in false data in select amounts. "Noise" is defined as data points, or entire fields of data, that do not actually correlate to an individual. The process of adding noise is also highly variable depending on the data collected, but the general principle involves "hiding" real personal information among randomly generated data that serves no actual purpose. When an organization seeds false data among real data, malicious actors are significantly hampered from using the data set for nefarious means or reverse engineering the above-mentioned anonymization techniques by using the data set as a whole. A newer method used by businesses called "differential privacy," discussed below, applies the practice of adding noise in unique ways to increase the security of personal information held by businesses.

Encryption

Encryption is an effective means of implementing the above-mentioned techniques. The process involves filtering collected data through an encryption algorithm that renders the data useless to a human reader, which can then be unscrambled using a private password. A common and easily used method is symmetric encryption, where data is hidden by an algorithm on collection and becomes readable only after inputting a private key password. Encryption comes in a variety of formats ranging from simple private key encryption to complex end-to-end encryption, but serves the common purpose of making the personal information collected by the business unreadable by malicious actors. Techniques like "salting and hashing" increase the difficulty of breaking the code. However, authorized analysts with a need to access the data set can reap the analytical benefits of the data with access to the decryption key.[2]

NEWER ANONYMIZATION AND MINIMIZATION TECHNIQUES

Federated Learning of Cohorts (FLoC)

FLoC is a combination of generalization, suppression, and adding noise that involves the collection of personal information and sorting it into anonymized cohorts by its identifying factors. Google implemented the technique as an alternative to third-party cookie tracking technology on

2. Of course, organizations must have strong internal security safeguards to ensure that such keys are not accessible to malicious internal or external actors.

their Chrome browser in March 2021. Cohorts are sorted by the types of internet activity that users have in common, serving as a method of generalization and suppression by providing advertisers with only the most pertinent data categories on an abstract level. Cohorts equally contain hundreds if not thousands of users, making any individual's behaviour difficult to associate back to a specific person.

FLoC has been deployed on Chrome browsers as a pilot project, resulting in a potential radical shift in the effectiveness of third-party cookies. Google's privacy sandbox provides the mechanisms behind FLoC on an open-source basis, permitting businesses the option of exploring whether FLoC could be of use for their own purposes. In principle, the technology behind FLoC could equally apply to businesses who are seeking to generalize personal information held to shield themselves from privacy breaches, resulting only in abstract cohorts rather than personally identifying information.

Tokenization

Tokenization is a more thoroughly applied method of encryption and masking that replaces personal information with a series of tokens that identifies specific pieces of personal information. The principle has already seen broad use in the payment processing industry, where credit card payment information has been tokenized to permit transfer requests between acquirer banks, payment networks, and issuer banks without revealing sensitive personal information during transfers.

Tokenization acts as a further step to masking by replacing the personal information values entirely. The process involves the use of a "token vault," which stores the core algorithm used to generate a variety of tokens. Personal information that is submitted to the business is stored in the token vault, and the token is then transferred for various purposes. Only once a request is made to the token vault can the token be exchanged for the personal information it represents. As the token itself has no intrinsic value, even if malicious actors could crack the encryption, the token would not subsequently reveal any personal information. As an added benefit, any request to exchange a token for the personal information it represents could be tracked by the business to facilitate the investigation of a privacy incident. Tokens are also frequently randomized every time they are entered, even if the underlying personal information remains the same.

Tokenization is often not implemented as a stand-alone security offering and is often frequently paired with other solutions.

The technology behind tokenization is a strongly proven concept, with consistent innovations due to the popularization of block chain technology. However, tokenization is often not implemented as a stand-alone security offering and is often frequently paired with other solutions to offer a more comprehensively secure privacy system. Depending on the type of personal information being processed and traded, tokenization can be an effective means of protecting the transfer of personal information.

Multiparty Computation (MPC)

Secure Multiparty Computation (or "split processing") is a cryptographic solution that permits the sharing of data

processing results while leaving the data used to produce those insights secret. Previously, this process required a "trusted third-party source" to act as an intermediary. The process involved two parties giving relevant data to a third party, who delivered the required insights without revealing to either what the values were, and delivering the results confidentially.

MPC cuts out the intermediary by emulating the third party through advanced cryptography. The result is that business insights can be accurately gained while never having access to the personal information that produces it, especially in relation to larger data sets. If used properly, MPC has the potential to provide businesses with a secure means of deriving data insights even when the operating environment poses serious privacy risks. One example is a case where a data exporter wants to process personal information jointly using two service providers in jurisdictions with limited legal protections for personal information. The data exporter can implement an MPC system where the two service providers process personal information simultaneously without ever having access to the specific data set in question.

If used properly, MPC has the potential to provide businesses with a secure means of deriving data insights even when the operating environment poses serious privacy risks.

Though MPC is a method that has existed for some time, its recent application into data protection strategies is in no small part due to international regulators recognizing its effectiveness as a privacy protection measure. The European Data Protection Board specifically identifies MPC as both an effective supplementary measure to protect data in non-EU jurisdictions, and speaks to its potential as a technology that applies for systems adhering to privacy by default standards. The International Association of Privacy Professionals reported that in the United States, public institutions implement MPC to protect federal databases, and the *Promoting Digital Privacy Technologies Act* identifies MPCs as a cryptography technique of note to be studied.

Differential Privacy

Differential Privacy is a technique that simplifies the process of adding noise to a data set for even authorized users. In this model, the database is segregated from the analyst, who cannot see the personal information collected by the business. When analysts seek to generate a conclusion from certain data values, they submit requests to an intermediary piece of software known as a "Privacy Guard." The Privacy Guard assesses the privacy risk associated with a given request, and adds random noise to compensate before returning a data value.

The result is that the value given back to the analyst is close enough to the real value to be useful, while at the same time sufficiently noisy to prevent any kind of reverse engineering that would expose an individual's personal information. Businesses have implemented the practice of differential privacy with some success, including Microsoft, Apple, and Google. By calibrating the amount of random noise added into the privacy risk, differential privacy can offer a comprehensive solution to retain analytical usefulness by shielding the true data values, but provide an accurate overall picture of trends within a data set.

Synthetic Data

Synthetic data is an addition to the above-mentioned practice of "Adding Noise." The general practice is the use of an algorithm that simulates the connections made through analysis of personal information, and reverse-engineers the conclusions to generate sets of dummy

data. MIT has released the Synthetic Data Vault to assist developers in this regard. In a test of the usefulness of insights drawn from the use of synthetic data when compared to actual datasets, researchers were capable of drawing accurate conclusions 70% of the time even while using synthetic datasets.

In principle, synthetic data methods could sidestep the use of personal information entirely. Businesses could draw useful insights and analytics from simulated customer behaviour, rather than exposing the business to privacy risks involved with collecting data from customers. However, synthetic data solutions are still in the early stages of implementation. Depending on the type of analytics a business is seeking to replicate, synthetic data could be a costly means of anonymizing data compared to the alternative methods mentioned herein.

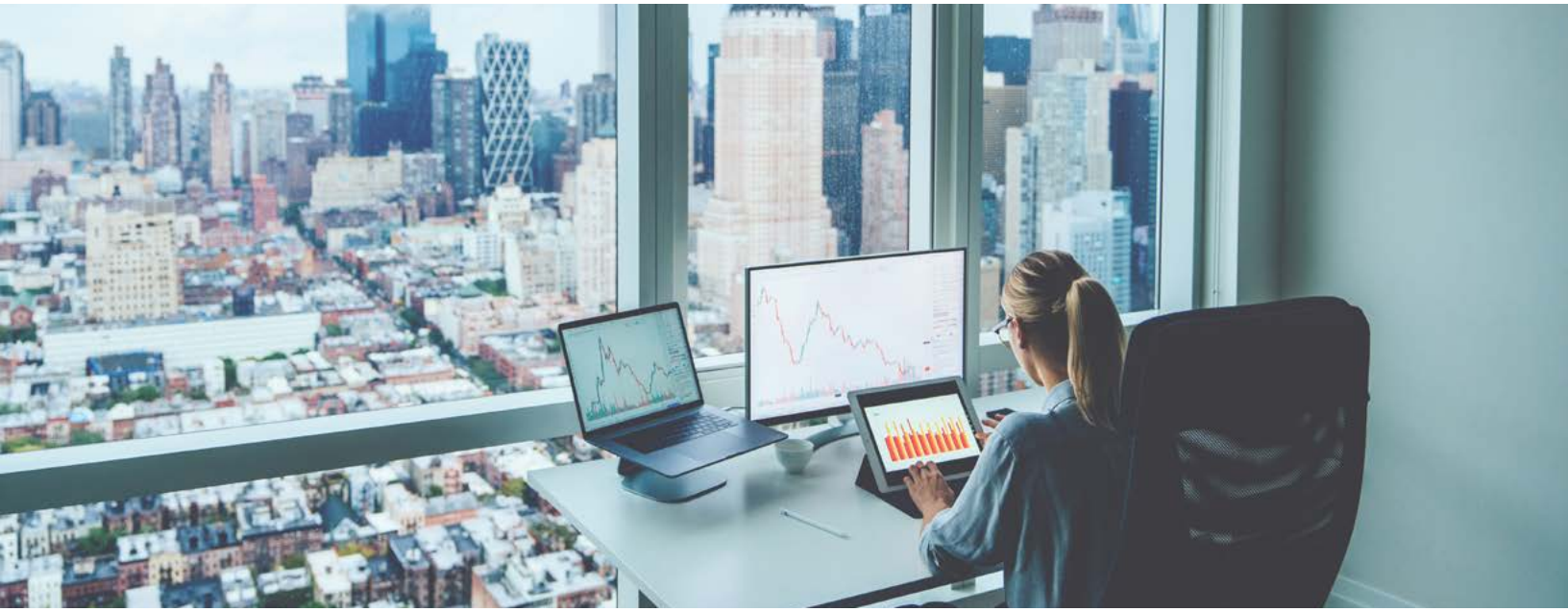
Universal ID

Universal ID technology is an applied use of both encryption and suppression, which identifies individual users by a generic username rather than collecting a broad spectrum of personal information for users online. The most prominent version of this technology is the open-source Unified ID 2.0, established by TradeDesk, and adopted by Buzzfeed, AMC Networks, Foursquare, Salon, and the LA Times. Universal ID involves an open-source, encrypted, and unique username for individuals who browse partner websites. Users who create a profile have their email addresses encrypted and tokenized (as explained above), and the universal ID token is traded between service providers and advertisers to provide targeted advertising to individuals without knowing many of the unnecessary particulars about the underlying individual that may leave them open to malicious actors.

Universal ID systems are not exclusive to the private industry, and the technology has seen successful application in the public sector. Examples include the ID Austria program, whose pilot phase concluded in autumn 2021. The system uses the same tokenization methodology to encrypt the personal information of Austrian citizens, who can now use the digital identifier as a means of accessing public services. Though universal ID systems are often discussed in the context of cross-business applicability, businesses with multiple parent or subsidiary service offering could also benefit from a unified ID system. An example in practice is the Universal ID offering by SAP, which unifies the service offerings to a single system.

CONCLUSION

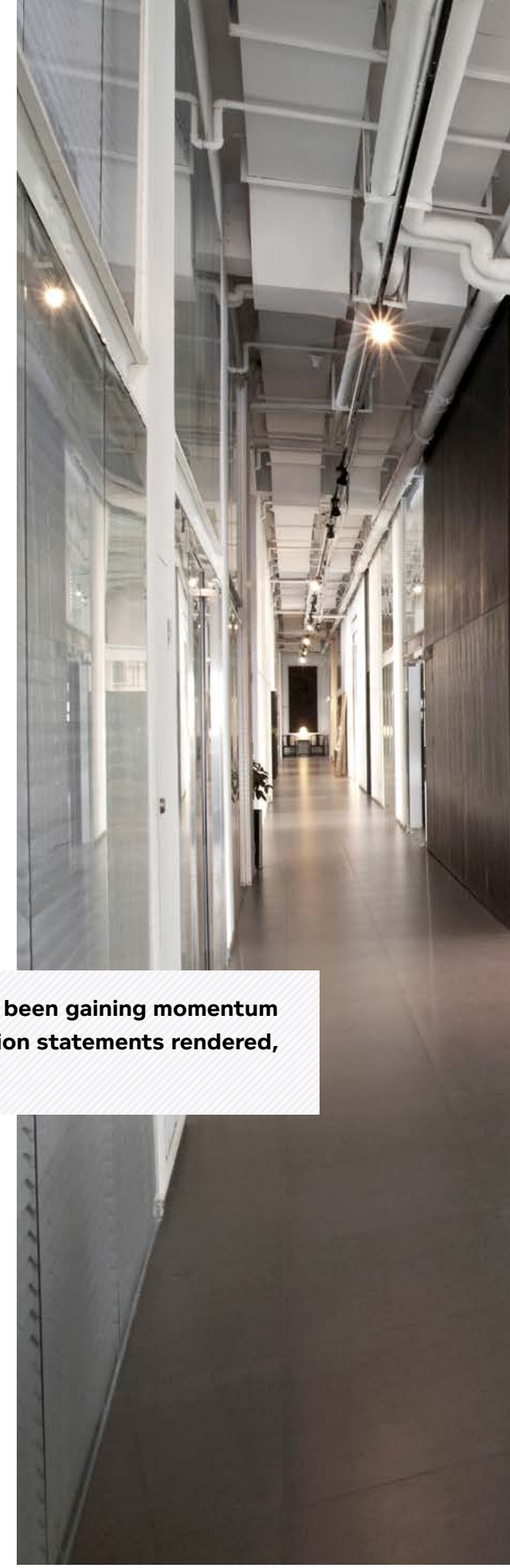
Personal information and data analytics are an essential part of the financial projections for many businesses worldwide. As regulators continue to clamp down and impose exacting standards on the processing of personal information, while potential penalties reach staggeringly high levels of revenues, strategic anonymization can offer practical benefits by actively reducing legal risks while preserving the usefulness of personal information. Businesses should consider the practical benefits of implementing one or more of the above-mentioned techniques in order to ensure compliance that is more effective without compromising the efficiency of business practices.



The (Digital) Enforcers: The Competition Bureau Takes on Big Tech

The regime change in the United States has ushered in a new era of antitrust activism. President Biden has signalled that enforcement against the so-called FAANGs will be a priority for his administration in the coming years, appointing high-profile, Big Tech critics like Lina Khan and Jonathan Kanter to take the lead on competition policy and enforcement for his administration. Given the countries' close economic ties and the United States' sphere of influence over Western economies, Canada's competition strategy will be necessarily informed by the United States and the Canadian Competition Bureau (Bureau) appears to be positioning itself for a stronger stance on digital enforcement.

Though not an entirely new phenomenon, the Bureau's scrutiny of technology and data industries has been gaining momentum in recent years, with several market studies published, position statements rendered, and investigations launched in the digital space. For example, in May of 2020, the Bureau reached a settlement with Facebook regarding its misleading privacy claims. Following an investigation that examined the social media giant's privacy practices, the Bureau determined that Facebook gave users the false impression that they could control who could see and access their personal information on the platform, despite Facebook sharing users' data with third-party developers in a manner inconsistent with its privacy claims. Accordingly, Facebook agreed to pay a C$9 million penalty and to cover the costs of the investigation.



The Bureau's scrutiny of technology and data industries has been gaining momentum in recent years, with several market studies published, position statements rendered, and investigations launched in the digital space.

Later that same year, the Bureau went public with its investigation into Amazon's conduct, examining whether Amazon employs restrictive trade practices in its Canadian marketplace, and whether these practices amount to an abuse of dominance. In particular, the Bureau is interested in any Amazon policies that may impact third-party sellers' willingness to offer their products for sale on other channels, the ability of third-party sellers to succeed on Amazon's marketplace without using its "Fulfilment By Amazon" service or advertising on the marketplace, and any efforts by Amazon to influence consumer to purchase their products over those offered by third party sellers. It appears that this investigation is ongoing, though no further updates have been released.

The Bureau has also focused on digital enforcement outside of Big Tech. Driven by the onset of the pandemic, digital health care has remained a banner cause for the Bureau, launching a public consultation in 2020 to assess

any impediments to access, competition and innovation in the sector. Initial feedback from key stakeholders, such as health networks, regulators, professional associations, and digital health-care providers, was published in 2021. Stakeholders flagged the lack of interoperability between providers (raising privacy implications), challenges relating to remuneration, and issues regarding procurement and commercialization processes for health technologies in Canada.

Developments this fall signal that the Bureau's digital enforcement strategy will only pick up steam. On October 22, 2021, the Bureau obtained a court order to advance its civil investigation into conduct by Google relating to its online advertising business. The Federal Court of Canada granted the Bureau's request to force Google to produce records and written information on its display advertising business in Canada. Though little has been made public, it appears that the Bureau is attempting to discern whether Google's practices have impeded the success of competitors in online display advertising, resulting in high prices, reduced choice, and/or hindering of innovation for ad tech services — ultimately harming advertisers, publishers, and consumers. The Bureau's investigation is ongoing.

That same month, in his address at the Canadian Bar Association's competition law conference, the Bureau's Commissioner, Matthew Boswell, detailed the Bureau's plans for tackling concentration and anticompetitive conduct in digital economies. Pointedly titled "Canada Needs More Competition," Commissioner Boswell's speech emphasized the urgency of increasing Canada's enforcement of the *Competition Act* to assist with Canada's economic recovery post-pandemic and to keep up with the international shift toward more aggressive antitrust enforcement. Chief among the action items was increased digital enforcement and promoting compliance in the digital marketplace, where breaching antitrust laws has become merely the cost of doing business.

The Bureau has established a new Digital Enforcement and Intelligence Branch - envisioned to become the Canadian centre of expertise on technology and data issues.

The Commissioner's enforcement goals go hand in hand with the Bureau's increased budget. This includes money for the creation of a new Digital Enforcement and Intelligence Branch, led by Deputy Commissioner Leila Wright. This branch is envisioned to become the Canadian centre of expertise on technology and data issues, and act as an early-warning system for potential competition issues in the digital and the traditional economies. While it will not have its own cases, it will provide intelligence expertise and support to branches carrying caseloads, in addition to collaborating closely on the Bureau's advocacy and pro-competitive policy work.

Though the impact of the Bureau's digital enforcement strategies remains to be seen, it is apparent that the Bureau — along with its international counterparts — will be fixated on disciplining digital markets like Big Tech for the coming years.

Privacy Diligence in M&A

Where it was once unusual — and likely fruitless — to request comprehensive documentation about a target's cybersecurity practices during due diligence, the risk exposure from cybersecurity incidents and financial penalties for violating privacy legislation have resulted in changes to the old standard practices. Evaluating a target's compliance with applicable privacy legislation and its security posture is now part of standard due diligence reviews during M&A transactions; and it's here to stay.

Targets need to be prepared for comprehensive requests about their data practices and policies. Buyers need to ask the right questions and request the right documents.

THE FUNDAMENTALS

Every target is carrying some cybersecurity risk and buyers need to understand the details so they can understand, mitigate and allocate that risk. The risk could be as obvious as a publicly known data breach, or more surreptitiously woven throughout the target's entire operations as poorsecurity practices, inattention to privacy compliance and excessive indemnities and liability in commercial agreements. Buyers also need to know that the target has the necessary rights to use personal information as it has been doing and, if necessary, for the buyer's new plans for that personal information.

> **Every target is carrying some cybersecurity risk and buyers need to understand the details so they can understand, mitigate and allocate that risk.**

Class Actions and Litigation Risk: Buyers need to review documentation pertaining to past or pending claims, disputes, litigation or other proceedings by or against the target related to privacy, data, software, technology, or confidential information. Supporting documentation explaining the context surrounding such matters is crucial for a proper evaluation of the associated risks they may carry. The risk of class action lawsuits arising from data breaches and inappropriate use of personal information is significant.

Regulatory Fines: While regulatory fines used to be uncommon in Canada's ombudsperson model of privacy regulation, Québec's new privacy legislation (Bill 64) includes GDPR-style regulatory penalties of up to C$10 million or 2% of worldwide turnover, whichever is greater, and penal sanctions of up to C$25 million or 4% of worldwide turnover. Fines can double for repeat offenses. The Canadian federal government had also proposed a new privacy law, and while the bill is currently dormant, it had included administrative monetary penalties of up to the greater C$10,000,000 and 3% of the organization's gross global revenue and

potential fines up to the greater of C$25,000,000 and 5% of the organization's gross global revenue. Further, Ontario, Alberta and British Columbia are all at some stage of considering privacy law changes, so additional, overlapping fines may be coming.

Lawful Processing: Buyers need to understand what personal information the target processes and what legal grounds it is relying on so that the processing can continue going forward. Buyers may also have plans for processing the personal information in new ways. As Canadian privacy legislation is still consent-based, any ongoing or future processing must be consistent with the consent provided by the relevant individuals.

With the passing of Bill 64, in Québec consent must now be clear, free, informed, and provided for specific purposes.

POLICY AND SOP REVIEW

Use the life cycle of the data collected by an organization to inform your diligence checklist.

Privacy and Data Security Policy Checklist	
☐	Privacy Policies and Notices (including internal policies)
☐	Incident Response Plans
☐	Internal Data Incident Reporting Forms and Logs
☐	Information Security Policies and Subordinate Policies
☐	Data Retention Policies
☐	Data Destruction Policies
☐	Data Subject Access/Rights Request Policies
☐	Cyber Insurance Policies
☐	Contracts Affecting Cyber/Privacy Liability
☐	Business Continuity Plans
☐	Disaster Recovery Plans
☐	Statutorily Required Agreements, such as Data Processing Addenda and Business Associate Agreements

SECURITY AND DATA INCIDENT MITIGATION

Data breach procedures and records: As required under Canadian privacy laws, companies should have notification procedures for affected individuals and regulatory authorities, as well as records of security incidents. Identify any data security incidents or breaches involving the target's information technology infrastructure or its collection, use, storage, and transmission of personal or confidential information.

Certificates: Documentation related to industry standard certificates, such as the ISO 27001 and NIST, as well as information specific certificates, such as the PCI-DSS for payment card information if necessary, are useful preliminary markers that a target has implemented security safeguards for physical, technological, and organizational controls in a manner consistent with industry standards, as is required under Canadian law. Regardless of any acquired certificates, a complete operational due diligence review of a target's security posture may be necessary depending on the type of transaction.

Audits: Whether conducted internally or externally, audits can help pinpoint the level of risk that a Buyer is acquiring, which may be material for the transaction or used to inform their technology strategy following the deal. Results from

recent roundtable exercises and penetration testing may also prove useful to assess the target's security posture.

Cyber Insurance Policy: It is now typical for companies to have cyber liability insurance, but buyers need to understand the actual coverage and what claims the target has made under the policy to date.

THIRD-PARTY DATA TRANSFERS

Data Transfer and Privacy Provisions in Vendor and Customer Contracts: Does the target have contractual clauses in place to protect the personal information it collects and transfers to third parties for processing? What has the target itself agreed to with respect to safeguarding data provided to it? All material consumer and vendor contracts that provide for the transfer of personal information should be reviewed with these questions in mind.

In commercial agreements, there is still significant variability in cybersecurity and privacy indemnities, representations and warranties.

In commercial agreements, there is still significant variability in cybersecurity and privacy indemnities, representations and warranties. A target that processes personal information on behalf of its customers can have huge risk exposure if it has granted broad indemnities or not limited its liability.

CROSS-BORDER CONSIDERATIONS

Cross-border data transfers: Consider whether the transaction would be affected by recent provincial privacy legislation or EU case law governing cross-border transfers of personal information.

- **Bill 64:** Before transferring personal information outside of Québec, a privacy impact assessment must be conducted that takes into account the sensitivity of the personal information, the purpose for which it is to be used, safeguards, and the legal framework applicable in the receiving jurisdiction.
- **Schrems II:** The European Court of Justice's ruling in the Schrems II decision invalidated the EU/U.S. Privacy Shield. Now, companies wishing to transfer personal information from the EU to the U.S. need to complete a transfer impact assessment. Be on the lookout for customer and vendor contracts that result in personal information being transferred from the EU to the U.S.

Beware of CASL: International investors are often surprised to find that breaching Canada's anti-spam legislation (CASL) comes with fines of up to C$10,000,000. What you'll need:

- A copy of the Target's CASL policy;
- A description of how the target complies with CASL, particularly how Commercial Electronic Messages (CEMs) are sent, the recipients of CEMs, and unsubscribe mechanisms;
- Sample CEMs; and
- All CASL related complaints and notices from the government.

You can begin your CASL due diligence review before receiving these documents. For example, if a company's website users are asked to complete a form in order to join a mailing list, this is a good initial indication that the company seeks express consent in accordance with CASL. However, if a company's publicly facing "Contact Us" page includes a pre-checked consent box to subscribe to the Company's newsletter, this would violate CASL's requirement to acquire separate opt-in express consent before sending CEMs (unless exceptions are applicable).

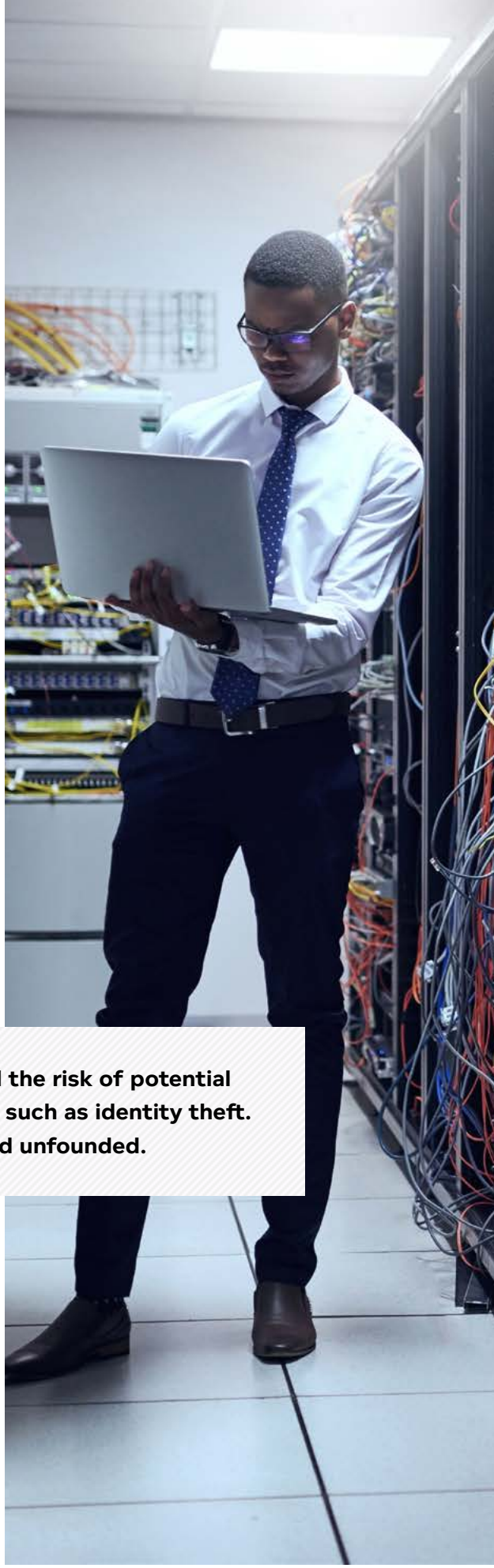
Data Breach Class Actions and Litigation in Canada

NEW CLASS PROCEEDINGS REGIME MAKES ONTARIO LESS POPULAR FOR PLAINTIFFS

In October 2020, amendments to the Ontario *Class Proceedings Act*, 1992 came into force, implementing a number of substantive and procedural changes that make it more difficult for plaintiffs to bring data breach class actions in Ontario.

The most significant substantive change to the legislation is a more rigorous test to be applied at certification. Influenced by the U.S. model, the preferableprocedure analysis now requires the plaintiff to prove that common issues predominate over individual ones, and that a class proceeding is superior to all reasonably available means of determining the entitlement of the class members to relief or addressing the defendant's impugned conduct. This is in contrast to the old test (and the test that remains in many other provinces) that only required that there exist some common issues whose resolution would advance the litigation. The amendments also impose procedural changes that could make it more difficult for plaintiffs to advance claims in Ontario, such as a new presumption that defendants' dispositive motions can proceed before a plaintiff's motion for certification.

Overall, these amendments make Ontario a less attractive forum for plaintiffs seeking to bring class actions arising from a data breach. As many predicted, the year after the Ontario amendments came into force has brought with it a noticeable shift, with more plaintiffs seeking to bring their class actions in common law jurisdictions other than Ontario, such as B.C. and Alberta.



Plaintiffs often claim damages for anxiety, inconvenience, and the risk of potential future misuse of their information arising from a data breach, such as identity theft. However, increasingly, such claims can seem opportunistic and unfounded.

COURTS BEGIN TO GROW SKEPTICAL OF DATA BREACH CLASS ACTIONS; REINFORCE THE IMPORTANCE OF POST-BREACH MITIGATION

While plaintiffs continue to file litigation — often class action litigation — in the wake of data breaches, there is a real question as to whether the actual or potential release of personal information has *actually* caused any harm to affected individuals. Over the past year, courts have begun to look critically at plaintiffs' claims of minimal or speculative harm.

Plaintiffs often claim damages for anxiety, inconvenience, and the risk of potential future misuse of their information arising from a data breach, such as identity theft. However, increasingly, such claims can seem

opportunistic and unfounded. Cyber attacks and the resulting potential loss of data are now widely viewed as commonplace, not an exception. And many companies respond to breaches by offering services such as credit monitoring to reduce the risk of future harm. By the time a proposed class proceeding winds its way through the courts, there is often little or no evidence that any of the proposed class members has actually suffered a loss.

Canadian courts scrutinized data breach claims, and in many cases either dismissed or refused to certify them if there was no evidence that class members actually suffered any compensable harm.

In 2021, Canadian courts scrutinized data breach claims, and in many cases either dismissed or refused to certify them if there was no evidence that class members actually suffered any compensable harm. For example:

- In *Lamoureux v. Investment Industry Regulatory Organization of Canada (IIROC)*, the Québec Superior Court dismissed an authorized class proceeding on the merits because the plaintiff had failed to establish any harm above ordinary annoyances, finding that such everyday anxieties and annoyances are not compensable.
- In *Setoguchi v. Uber B.V.*, the Alberta Court of Queen's Bench took heed of its gatekeeper role and the culture shift away from certifying de minimus claims, and declined to certify a class action arising out of a data breach. There was no evidence class members had suffered harm or loss — indeed, there was positive evidence that no class member had. And even if some class members had suffered a loss, a multitude of individual hearings would be required to establish causation and damages, making a class proceeding inappropriate.
- In *Simpson v. Facebook* and *Kish v. Facebook*, the Ontario and Saskatchewan courts refused to certify a class action about the Cambridge Analytica data breach because there was no evidence that Canadian Facebook users' personal data was inappropriately shared, and therefore there were no common issues related to breach of privacy that could be certified.
- In *Kaplan v. Casino Rama Services Inc.*, the Ontario Superior Court of Justice refused to certify a class action because there was no evidence anyone had suffered any harm, including because of the defendant's exemplary incident response. It had "contacted all appropriate authorities, took steps to close down the two websites that contained the stolen information, notified the thousands of customers, employees and suppliers potentially affected by the security breach and offered free credit monitoring services for one year to many of them."

Looking forward, defendants who are victims of a cyber attack can expect to place more emphasis on the absence of harm to class members, as well as on the robustness of their incident response and measures to reduce risk of harm to would-be plaintiffs, as a means to defend against class actions.

PRIVILEGED? THE DEBATE OVER FORENSIC INVESTIGATION REPORTS

Lawyers advising companies in the wake of a data breach usually engage cyber forensic experts to investigate the incident and produce a report for use by legal counsel. Such reports are essential for lawyers to provide candid legal advice to their clients about the breach and related litigation and are intended to be privileged and confidential. However, plaintiffs and organizations may still try to compel production of the report in litigation or regulatory investigations.

Lawyers advising companies in the wake of a data breach usually engage cyber forensic experts to investigate the incident and produce a report for use by legal counsel.

A number of recent U.S. decisions have confronted this issue, and these decisions show that, in some circumstances, forensic reports may be vulnerable to attacks on their privilege if appropriate protective measures are not taken. For example, in *In re Capital One Customer Data Security Breach Litigation*, a Virginia court ruled that a forensic investigation report was not privileged because it was not created for the purpose of litigation: the forensic investigator who prepared it was previously engaged by the company under a non-privileged engagement and, even though the company's lawyers executed a new engagement letter with the investigators after the breach, it was for the same scope of work. The court further found that, even if the report had been privileged, the privilege was waived when the company disclosed its contents to the company's auditor, regulators, and other business personnel. Similarly, in *In re Rutter's Data Security Breach Litigation*, a Pennsylvania court found that an investigation report was not privileged because it was prepared for the purpose of determining whether a breach had occurred — not for defending the company in litigation.

The U.S. decisions, while based on U.S. privilege laws, foreshadow an issue that may increasingly find its way into Canadian courts. For example, in *Kaplan v. Casino Rama Services Inc.*, the Ontario Superior Court of Justice found that the company waived privilege over portions of forensic investigation reports prepared in the wake of a data breach when it disclosed the number of people affected by the breach.

Going forward, organizations should anticipate that regulators or plaintiff's counsel may seek disclosure of investigation reports and challenge any privilege claimed over them. Companies should act accordingly to protect privilege. This includes working with legal counsel to establish an incident response plan and strategy for preserving privilege, over forensic investigation reports and generally. Ensuring that counsel are involved, and that expert mandates are properly structured to prevent loss of the privilege that attaches to them, is likely to become increasingly important.

TRENDS IN CYBER INSURANCE

Insurers Crack Down on Cyber Coverage

Having insurance coverage for litigation and incident response costs in the event of a data breach continues to be an important means of managing risk. However, the move to remote work during the COVID-19 pandemic and the flood of cyber attacks that followed have made cyber policies extremely expensive for insurers. Not surprisingly, the last 12 months have seen insurers rapidly adjusting their insurance approaches and offerings.

First, it is becoming more and more commonplace for insurers to offer cyber-specific policies and to refuse coverage for cyber incidents under general commercial and other non-cyber policies. Many insurers — in an effort to preclude so-called "silent" cyber coverage — have inserted "data" exclusions in their non-cyber policies. In *Family and Children's Services of Lanark, Leeds and Grenville v. Co-operators General Insurance Company*, the Ontario Court of Appeal

broadly interpreted one such "data" exclusion clause in a commercial general liability policy, and held that it did indeed exclude coverage for litigation related to a data breach.

Looking forward, it will be risky for companies to rely on non-cyber policies to provide coverage for cyber attacks and data breaches. The ruling in Co-operators signals a judicial shift in the interpretation of non-cyber insurance policies in favour of excluding coverage for data breaches. While some general liability, directors and officers, and other insurance policies may still provide data coverage based on their specific language, having an adequate cyber-specific policy is and will continue to be the best practice.

Insurers are paying closer attention to the IT security questionnaires policyholders must complete when applying for or renewing cyber insurance.

Second, insurers are paying closer attention to the IT security questionnaires policyholders must complete when applying for or renewing cyber insurance. Going forward, companies can expect insurers to demand more detailed and comprehensive questionnaires, or even require policyholders to have or implement certain data security hygiene measures to secure coverage at all. These questionnaires are important; insurers may rely on any mistaken or incomplete answers to negate or limit coverage when an incident happens. Companies should invest time to provide accurate and comprehensive answers to the insurer's questionnaire to avoid potentially jeopardizing coverage.

Maintaining Control Over Selection of Service Providers

With the rise of cyber-specific insurance policies, insurers are increasingly likely to require policyholders to obtain approval for any third-party service providers they engage for the breach response — or even require policyholders to select from a list of third-party service providers selected by the insurer. However, third-party service providers like external legal counsel and forensic investigators are an integral part of a company's breach response. Being able to pick the service providers the company wants to work with, and mobilize them immediately, can be a critical component of an incident response plan. Policyholders should expect it to become increasingly important to check their insurance policies for any service-provider restrictions and approval requirements, and to negotiate approval of their preferred service providers when securing or renewing their policy (not in the wake of a breach).

Ransomware Attacks: Strategies for Preparation and Mitigation

Businesses' dependence on (and investment in) online infrastructure resulting from the COVID-19 pandemic, and the availability of cryptocurrency, has created an environment ripe for significant increases in the frequency and ingenuity of ransomware attacks. As the workplace continues a long-term transformation, flexible work arrangements and remote access to company data are likely to continue to provide malicious actors with ample targets. Not unlike other criminal enterprises, cybercrime continues to become more sophisticated and "businesslike" in its application.

Over the past year, these developments in ransomware — alongside a number of very prominent breaches in the public and private sectors — have prompted international concern regarding cybercrime, and are likely to generate more political willpower and co-ordinated strategies to combat ransomware in the near future. Political and business actors in Canada, including the Chamber of Commerce, are also alive to these concerns. These events make responding to an attack incredibly complex and time-sensitive, as domestic or foreign government sanctions aimed at ransom groups and virtual currency exchanges can derail a negotiation in midstream.

Strategies to combat cybercrime, regulate cryptocurrency, and obtain global relief notwithstanding traditional jurisdictional boundaries are still in their relative infancy. Businesses should be cognizant that legal frameworks in this area are unsettled, and will shift with some degree of frequency, sometimes in a way that could disrupt recovery from a ransomware attack.

Strategies to combat cybercrime, regulate cryptocurrency, and obtain global relief notwithstanding traditional jurisdictional boundaries are still in their relative infancy.

RANSOMWARE DEFINED

Ransomware is malicious software, or "malware," that prevents access to data, holding such data hostage until the target pays a ransom. Most often, ransoms are paid in a form of cryptocurrency, such as bitcoin.

Ransomware comes in two primary forms: (i) encryption ransomware, where data is encrypted, and a key to unlock the encryption is provided to the target upon paying the ransom; and (ii) lock-screen ransomware, where the target is locked out of their computer system or online device until the ransom is paid.

These methods are often utilized in concert with other strategies in order to achieve double or triple extortion, namely the levying of threats to release sensitive data exfiltrated in a ransomware attack, or

to directly target and harm individuals or customers whose data was stolen. These additional threats allow criminals to extract a larger fee from the target than they might have otherwise received for decryption alone.

There is also a possibility that, once an initial ransom is paid, there may be additional levels of encryption, or lock-screens, prompting additional ransom payments. However, the criminals behind the larger ransomware groups are generally cognizant that they command a "brand premium," as long as they maintain a reputation for keeping their word. A party that promises to decrypt data, and then doesn't, is unlikely to be trusted by the specialized service providers who assist businesses in these areas.

CURRENT TRENDS IN RANSOMWARE

The evolution of ransomware is a fascinating example of innovation in the criminal underground: just as other businesses diversify, so do cybercriminals. Cybercriminals are sensitive to changes in technology and market demands; and they continue to evaluate the effectiveness and efficiency of their products and gain inspiration from their competitors.

The *industry* of ransomware is an extreme form of entrepreneurial tech disruption, not entirely dissimilar from how Napster and Pirate Bay disrupted the creative industries via copyright infringement at an unprecedented scale. It is not a coincidence that ransomware actors use Megaupload/Mega — a service famous for facilitating mass copyright infringement — to make off with stolen company files, or that peer-to-peer systems are being used to distribute malware and infect unwitting users.

For example, in recent years, we have seen cybercriminals shift away from their nascent strategies, which centred around high-volume attacks, to a more selective approach, targeting larger businesses in an attempt to demand larger payments. As a rule, cybercriminals will gain access to, and then engage in reconnaissance *within* a target's data (such as their financial statements) before the actual attack in order to tailor their ransom request and to attempt to more effectively encrypt backup systems. Cybercriminals are also increasingly targeting smaller municipalities and health-care organizations, due to the perception that they have weaker security controls and are more likely to pay ransoms in order to restore essential public services — particularly during the COVID-19 pandemic.

Concurrently, the development of ransomware as a service (RaaS) has also changed the ransomware landscape significantly, becoming the most prevalent means of attack (Sophos 2022 Threat Report). Criminals can purchase monthly subscriptions to access user-friendly ransomware kits on the Dark Web, often complete with technical support. Instead of purchasing monthly subscriptions, some instead use a profit-sharing model, splitting the proceeds of ransoms with the RaaS provider. Some "providers" have invested in upscale graphic designs for their customer service portals and publishing portals.

These developments highlight three key take-aways: (i) cybercriminals are highly responsive to the nuances of current events, and will target vulnerabilities accordingly; (ii) diversification means that everyone, from individuals to medium-sized enterprises to large businesses may be subject to an attack in Canada; and (iii) ransomware is constantly evolving, meaning that strategies to prevent or react to ransomware require diligent upkeep.

HOW TO PREPARE FOR OR MITIGATE THE EFFECTS OF A RANSOMWARE ATTACK

The wide range of targets and immense potential costs of ransomware attacks highlight the importance of businesses investing in preventive measures. These include implementing strong security systems and procedures, rapidly patching vulnerabilities, engaging in penetration testing, educating employees on how phishing emails or other ransomware may be introduced into a system, reducing attack surfaces, air gapping backup data, building multiple layers of access within online data storage, and utilizing multi-factor authentication. The more difficult it is to navigate a system and the more difficult sensitive data is to reach, the less likely it is that cybercriminals will launch an effective attack.

Particular areas of vulnerability that should be addressed in preventive measures are backup storage, cloud storage, and remote access points. Frequent review of preventive measures is also essential — over time, cyber tools once reputed to be particularly secure become subject to the ingenuity of cybercriminals. For example, blockchain-based digital currencies and applications are increasingly subject to scams and hacks, and cloud storage is not invulnerable either. For more information, please see our article: Blockchain vulnerabilities — crypto hacks, blockchain forensics and legal challenges.

Even with robust preventive measures in place, it is equally important for business to have an incident response plan (IRP) in place for how to react in the event of a ransomware attack. Ransomware pop-ups (like the one shown below) are unsettling, and an IRP supports making measured and effective decisions, including when and how to involve legal counsel and external expertise. Additionally, having a well-formulated means of restoring from backup data in an IRP will help mitigate any reputational damages that may flow from the ransomware attack. For more information, please see our article: Ransomware: avoidance and response.

Figure 1 (Source: More Ransomware-as-a-Service Operations Seek Affiliates (bankinfosecurity.com))

In developing an IRP, businesses should also consider the key factors driving whether or not to pay potential ransoms. While paying ransoms may be the only method to recover data, businesses should take note that paying ransoms may make their business a target for future attacks. Payment could also result in violating sanctions, particularly with respect to the United States. Further, insurance providers may not cover the costs of paying the ransom, or other costs related to ransomware attacks, and data may remain compromised or corrupted even after the ransom is paid.

FUTURE TRENDS IN RANSOMWARE

In the near future, there is likely to be greater regulation, international co-operation and enforcement in the areas which coalesce with ransomware, including cryptocurrency and cryptocurrency exchanges, and money laundering. Already, there have been some examples of successful enforcement against cybercriminals and seizure of the proceeds of ransomware[3], as well as civil cases where the target of an attack was able to recover stolen cryptocurrency. In the next few years, law firms may be able to step up from their current dominant role as breach coaches and regulatory interfaces and win back ransom funds through innovative court proceedings using newer *Norwich Pharmacal, Bankers Trust, Mareva* and proprietary injunction remedies developed in recent cases to track and freeze ill-gotten gains. For more information, please see our article: Blockchain vulnerabilities – crypto hacks, blockchain forensics and legal challenges.

At the same time, business should be aware that cybercriminals will continue to modify their weapons to evade enforcement and target vulnerabilities. This means that businesses should continue to monitor trends in ransomware and update and test preventive measures and IRPs accordingly.

3. For example, please see US charges two men over ransomware attacks, seizes $6M | nypost.com, U.S. charges Ukrainian and Russian in major ransomware spree, seizes $6 mln | Reuters, and Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside | OPA | Department of Justice

Finding Value in Cyber Insurance

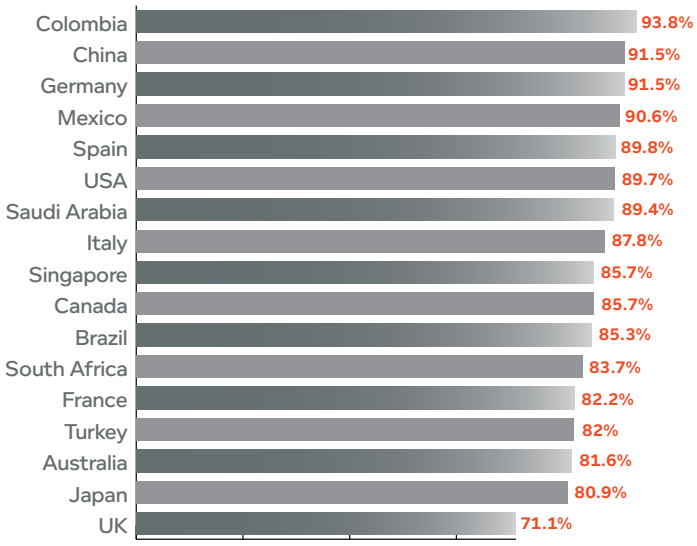
THE RISE OF CYBER CRIME TARGETING ORGANIZATIONS

As the world goes digital, insurance is increasingly being relied on to manage risk. The COVID-19 pandemic accelerated the digitization of many industries. Along with this transformation came an increase in system-wide cyber vulnerabilities as employers adapted to remote or hybrid work arrangements. The 2021 Hiscox Cyber Readiness Report (2021 Hiscox Report) of over 6,000 organizations across the U.S. and seven European countries found that 43% of respondents reported one or more cyber attacks in 2021. While increased spending on cyber budgets made larger organizations with over 1,000 employees more resilient, they were also the subjects of more attacks than their smaller counterparts.

Notably, a key change in the last year has been the increase in collective attack surfaces with the adoption of work-from-home and Bring Your Own Device policies. The 2021 Hiscox Report found that over half of employers are working remotely at least part time, requiring IT security teams to prioritize the security of distributed workforces, and that mobile devices have proven to be among the most difficult technologies to secure in adapting to these policies.

Cyber events are difficult to anticipate and budget for, as indicated by the statistics from the 2021 Hiscox Report. The average cost of cyber incidents for large organizations was higher than the combined average cost for medium and small organizations. Costs of cyber attacks ranged based on impact, making them unpredictable to plan for financially. One-in-ten organizations targeted paid a substantial fine that significantly impacted their bottom line. Of the one-sixth that were hit with a ransomware attack, over half paid a ransom to recover data or avoid publication of data. Canadian underwriters recognize that cyber threats are becoming more sophisticated and far reaching through the use of automation.

Canadian organizations were not spared. Coalition Canada, a cyber insurer, reported that the size of the average ransom demand its Canadian policy holders reported nearly tripled since early 2020. Ransomware has become one of the main contributors to a hardening of the Canadian cyber insurance market. Approximately 61% of Canadian organizations were impacted by ransomware attacks in the last 12 months (2021 Cyberthreat Defense Report). The average remediation costs for Canadian organizations that experienced ransomware attacks, including paid ransoms, was US$1.92 million (Sophos 2021 State of Ransomware). Cyber criminals justify greater demands by taking the cyber operations of organizations hostage until paid.



Percentage compromised by at least one successful attack in the past 12 months, by country

Source: 2021 Cyberthreat Defense Report, CyberEdge Group, LLC.

THE HARDENING OF THE CYBER INSURANCE MARKET

The demand for affirmative cyber insurance coverage has skyrocketed as a result of an evolving cyber threat climate. With rising demand, premiums for cyber insurance have also increased substantially and are expected to continue rising. According to S&P Global Ratings, premiums could increase by as much as 100% by 2023. The Canadian federal Office of the Superintendent of Financial Institutions (OSFI) recently reported on the Q2 2021 cyber insurance activities of the P&C insurers it regulates. The report found an almost 113% loss ratio for insurers with respect to cyber liability — many insurers are losing money under the present policy terms and premiums.

Stand-alone cyber policies allow insurers to carefully define coverage and work alongside clients to improve their cyber readiness. Many Canadian cyber insurers have adjusted their policies to include sub-limits and co-insurance. Insurance underwriters are furthermore rethinking the standard considerations on which cyber premiums used to be assessed. Many insurers in Canada and abroad are beginning to penalize companies that fail to demonstrate they have resilient cybersecurity measures in place (Howden Cyber Insurance: A Hard Reset).

IS CYBER INSURANCE IMPLIED IN GENERAL INSURANCE?

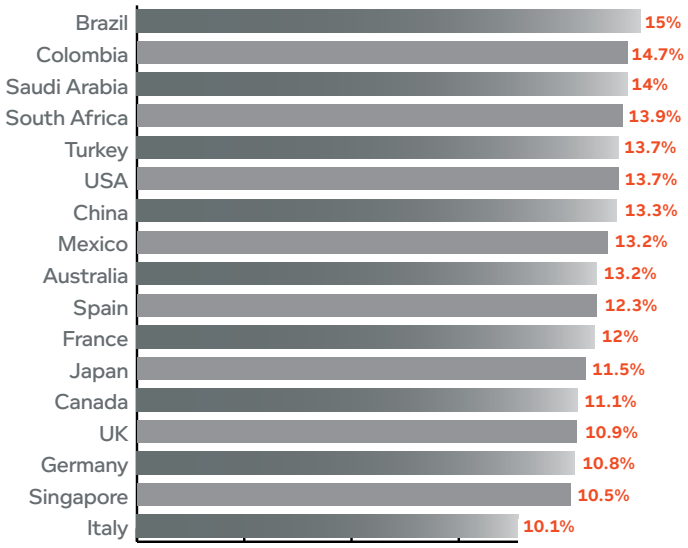
'Silent cyber' (also known as 'nonaffirmative cyber coverage') refers to the implied coverage of cyber risk by property loss and general commercial liability insurance. It represents a major source of uncertainty for insurers. As insurers are rolling out affirmative cyber coverage in stand-alone policies, some are fighting silent cyber claims under non-cyber policies.

In *Family and Children's Services of Lanark, Leeds and Grenville v. Co-operators General Insurance Company*, the Ontario Court of Appeal addressed a dispute over silent cyber insurance policy coverage. A breach of the portal managed by a family and children's services office led to the theft and public distribution on Facebook of confidential reports on 285 people. The insurer denied any duty to defend the office and its communications service provider against a C$75 million class action resulting from the data leak. It pointed to the data exclusion clause in the insurance policy, which excluded coverage for any claim related to "data." The Court unanimously determined that the exclusion cause unambiguously covered the data breach and leak in question, effectively excluding all cyber claims. This represents a shift in the interpretation of such exclusion provisions by Canadian courts. It is therefore best practice for Canadian organizations to acquire stand-alone, affirmative cyber insurance policy coverage. Yet one barrier to qualifying for an affordable cyber insurance policy is a lack of cybersecurity infrastructure.

One barrier to qualifying for an affordable cyber insurance policy is a lack of cyber security infrastructure.

The cybersecurity of many Canadian companies is inadequate. For this reason, many companies are likely to be charged higher premiums, if not denied cyber insurance altogether. Canadian organizations allocate among the lowest percentage of their operating budgets to cybersecurity of any developed country. According to the 2021 Cyberthreat Defense Report, Canadian organizations spent, on average, 11.1% of their IT budgets on cybersecurity. This is far below the global average of 12.7%. While there is a steady increase in this budget

allocation each year, Canadian companies must become more intentional about cybersecurity to avoid falling behind.



Percentage of IT budget allocated to security, by country.

Source: 2021 Cyberthreat Defense Report, CyberEdge Group, LLC.

Despite the pandemic forcing many small businesses to go at least partially digital, the statistics on this category of organizations are even more concerning. Only 24% of small businesses have some form of cyber insurance, with only 15% having a stand-alone policy. Over half of small businesses have no intention of purchasing cyber insurance within the next year. Small businesses that allocate funds to cybersecurity allocate, on average, 21% of their annual budget. Yet 47% of small businesses did not set aside any money for cybersecurity in 2021. This number is up from 33% in 2019, indicating small businesses are growing complacent despite becoming increasingly digital. Given the legitimate concerns of cyber insurers, the first step for these organizations will be to implement cybersecurity policies and practices.

Canadian organizations should be mindful of several considerations when shopping for a cyber insurance policy. First and foremost, ensure that the policy provides the coverage needed by scrutinizing the scope of the terms and the breadth of exclusions. After deciding on a policy, qualifying for, and complying with the terms, largely depends on the organization. Underwriters will assess premiums based on the cyber readiness of the organization as indicated per questionnaire answers. Organizations should therefore invest time in answering such questions carefully and thoroughly, updating the insurer regularly. If they have preferred third-party service providers, they should get them approved with the insurer. This avoids getting locked into using one of the insurer's pre-selected service providers as a condition of policy coverage. Once the policy is active, avoid automatic renewal without asking about coverage changes or enhancements. For more information, please see our article: Getting Cyber Insurance Right: 5 Practical Tips.

FOR MORE INFORMATION, PLEASE CONTACT:

Dan Glover
Co-Leader,
Cyber/Data Group, Partner
dglover@mccarthy.ca
416-601-806
TORONTO

Charles Morgan
Co-Leader,
Cyber/Data Group, Partner
cmorgan@mccarthy.ca
514-397-4230
MONTREAL

Michael Scherman
Technology, Partner
mscherman@mccarthy.ca
416-601-8861
TORONTO

Gillian Kerr
Litigation/Class Actions,
Partner
gkerr@mccarthy.ca
416-601-8226
TORONTO

Hovsep Afarian
Insurance, Partner
hafarian@mccarthy.ca
416-601-7615
TORONTO

Nikiforos Iatrou
Competition, Partner
niatrou@mccarthy.ca
416-601-7642
TORONTO

Isabelle Vendette
Privacy, Preparation
& Response, Partner
ivendette@mccarthy.ca
514-397-5634
MONTREAL

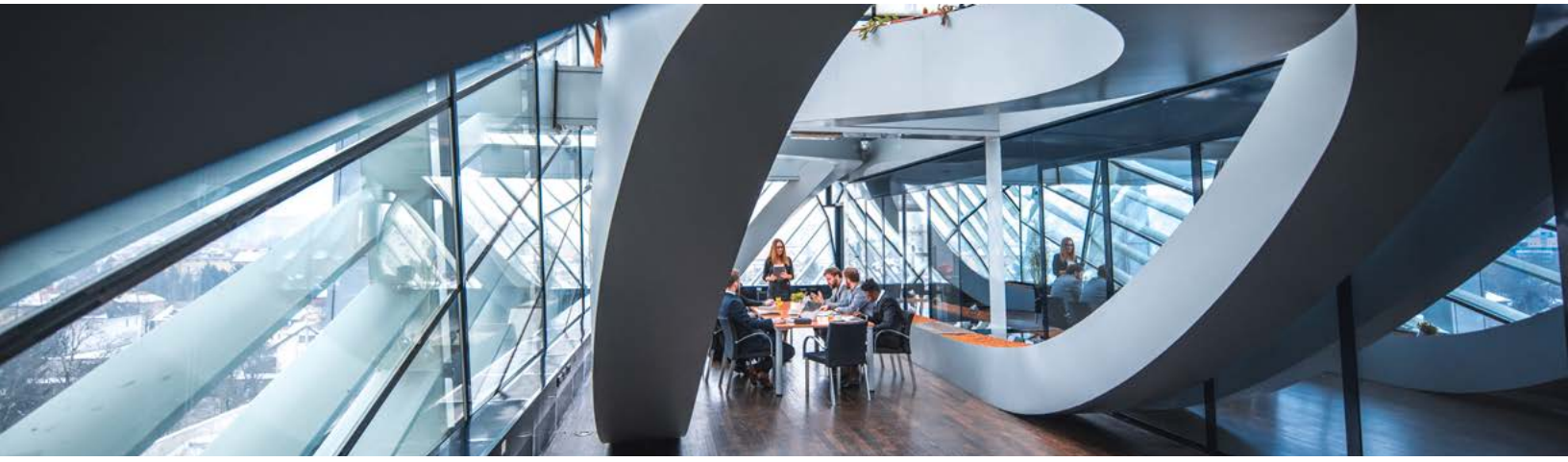
Jade Buchanan
Privacy, Preparation
& Response, Partner
jbuchanan@mccarthy.ca
604-643-7947
VANCOUVER

Katherine Booth
Preparation & Response,
Litigation/Class Actions,
Partner
kbooth@mccarthy.ca
604-643-7198
VANCOUVER

Justine Lindner
Labour & Employment,
Partner
jlinder@mccarthy.ca
416-601-8214
TORONTO

A SPECIAL THANKS TO

Marissa Caldwell, Ellen Chen, Jon Jacob Adessky, Erin Keogh, Cassidy Bishop, Kelsey Franks, Ella Hantho, Philippe April, Madison Howell, Todd Pribanic White, Loic Turner, Heather Mallabone, Rachael Carlson, Daniel Moholia



Get in touch

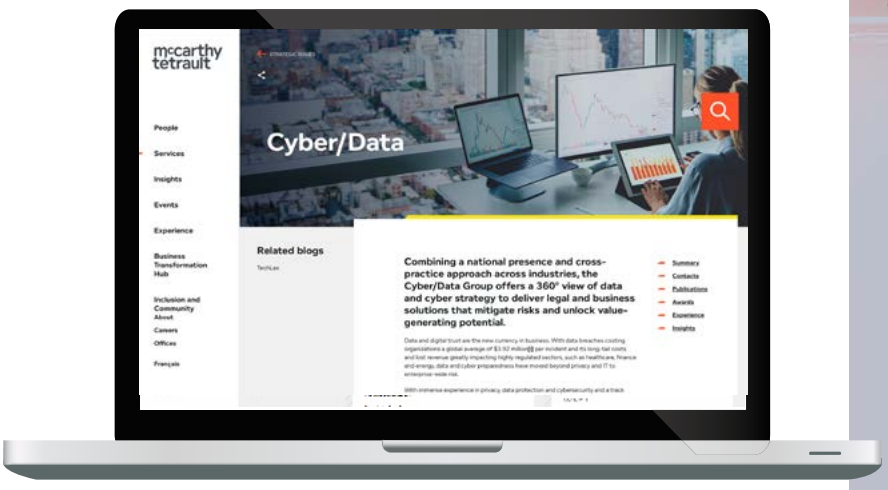
Combining a national presence and cross-practice approach across industries, the Cyber/Data Group offers a 360° view of data and cyber strategy to deliver legal and business solutions that mitigate risks and unlock value-generating potential. Our integrated multidisciplinary team works seamlessly across borders, advising global organizations through some of the largest cybersecurity incidents and regulatory investigations in Canadian history and is changing the state of Canadian privacy, cybersecurity and data law like no other firm.

About McCarthy Tétrault

McCarthy Tétrault LLP provides a broad range of legal services, providing strategic and industry-focused advice and solutions for Canadian and international interests. The firm has substantial presence in Canada's major commercial centres as well as in New York City and London.

Built on an integrated approach to the practice of law and delivery of innovative client services, the firm brings its legal talent, industry insight and practice experience to help clients achieve the results that are important to them.

FOR MORE INFORMATION, PLEASE CONTACT THE CYBER/DATA GROUP AT McCARTHY TÉTRAULT



mccarthy tétrault

VANCOUVER
Suite 2400, 745 Thurlow Street
Vancouver BC V6E 0C5

CALGARY
Suite 4000, 421 7th Avenue SW
Calgary AB T2P 4K9

TORONTO
Suite 5300, TD Bank Tower
Box 48, 66 Wellington Street West
Toronto ON M5K 1E6

MONTRÉAL
Suite 2500
1000 De La Gauchetière Street West
Montréal QC H3B 0A2

QUÉBEC CITY
500, Grande Allée Est, 9e étage
Québec QC G1R 2J7

NEW YORK
55 West 46th Street, Suite 2804
New York, New York 10036
United States

LONDON
1 Angel Court, 18th Floor
London EC2R 7HJ
United Kingdom