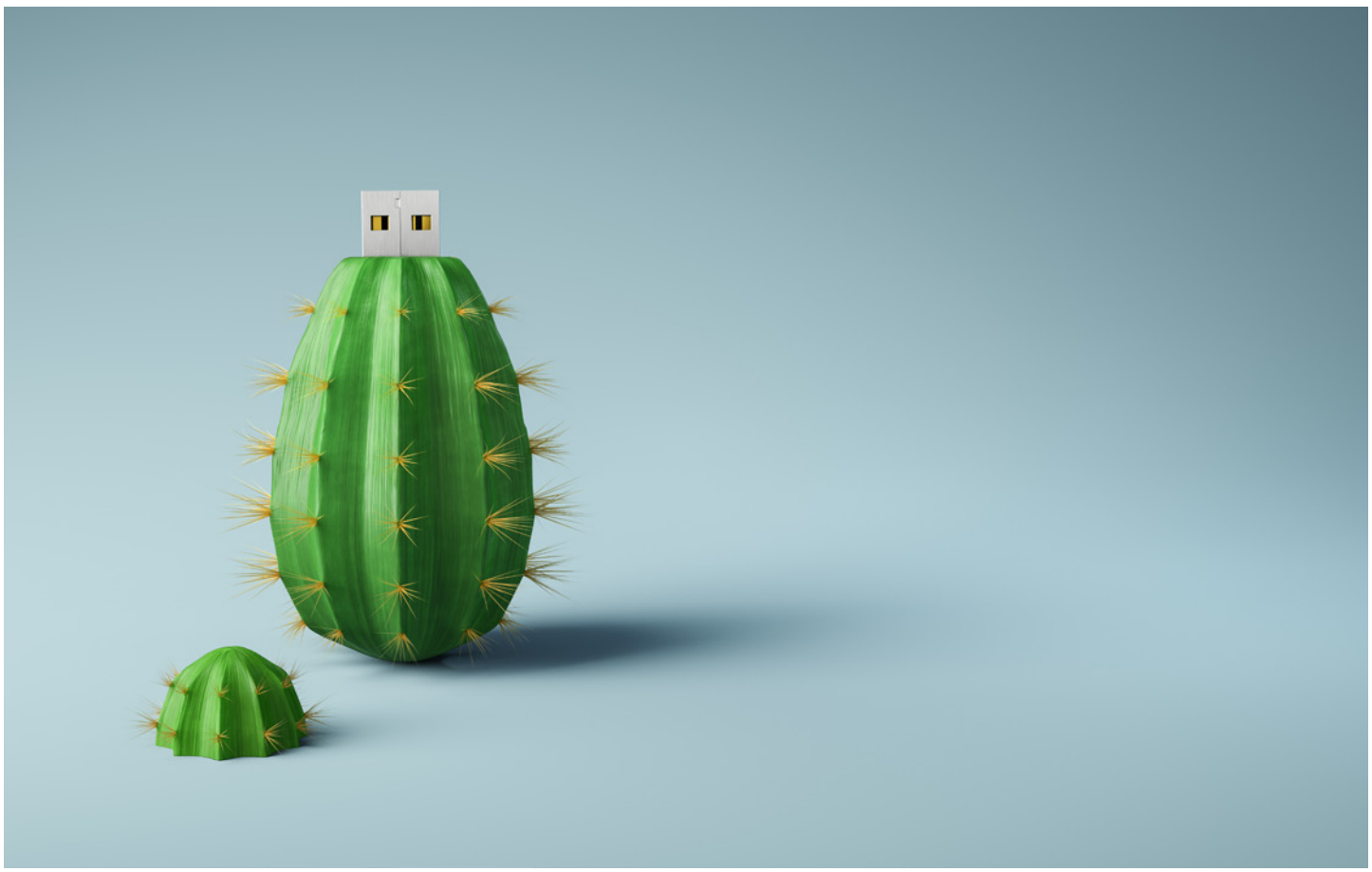
mcmillan

INDEPTH FEATURE Reprint August 2021

DATA PROTECTION & PRIVACY LAWS

Financier Worldwide canvasses the opinions of leading professionals around the world on the latest trends in data protection & privacy laws.



CANADA

McMillan LLP

Respondents

KRISTEN PENNINGTON
Partner
McMillan LLP
+1 (416) 865 7943
kristen.pennington@mcmillan.ca

Kristen Pennington is a partner at McMillan LLP, where she practices privacy and employment law. She counsels parties on a wide variety of privacy and data security issues, including employee privacy concerns, cross-border transfers of personal information and data breaches. She helps develop robust privacy compliance programmes, and drafts privacy policies, consent forms, acceptable use policies, and commercial privacy and data protection terms. She also assists vendors and purchasers with assessing the privacy law implications of corporate transactions.

MITCH KOCZERGINSKI
Associate
McMillan LLP
+1 (416) 865 7262
mitch.koczerginski@mcmillan.ca

Mitch Koczerginski is an associate at McMillan LLP, where he maintains a practice focused on retail and privacy issues. With a strong background in privacy law, he advises and represents clients in connection with privacy and data breaches involving payment card information, personal information, health information and sensitive business information. He routinely drafts and reviews privacy policies, conducts privacy and cyber security impact assessments and responds to access to information requests. He also handles submissions to provincial privacy regulators as well as the privacy commissioner of Canada on a variety of matters, including breach reporting and access to information appeals.

REPRINT

McMillan LLP

Q. Based on your experience, do companies in Canada properly understand their data protection duties? To what extent are you seeing rising awareness?

A. In our experience, Canadian companies are typically aware that there are laws governing their collection, use and disclosure of personal information, including requirements to implement appropriate safeguards to protect personal information. With that said, businesses are sometimes surprised by the broad application of Canadian privacy laws. Companies can also be under the misapprehension that their compliance with the European Union's (EU's) General Data Protection Regulation (GDPR) means that they are likely compliant with other international privacy laws. However, there are unique Canadian requirements that should form part of a global privacy compliance programme. We are currently observing increased awareness about privacy law compliance, as both the federal and some provincial governments are proposing significant overhauls to privacy legislation. At the federal level, a proposed law is currently being debated and, if passed, would introduce a host of changes to federal privacy legislation, including fines of up to the greater of $25m and 5 percent of the organisation's gross global revenue in the prior financial year. Amendments to the Province of Quebec's private sector privacy legislation have also been proposed, and the Ontario provincial government has recently indicated that it may introduce its own private sector privacy law.

Q. When companies undertake data processing activities – including handling, storage and transfer – what regulatory, financial and reputational risks do they need to manage?

A. Companies must understand which privacy laws apply to their data processing activities. Canada has a patchwork of privacy legislation, including the federal Personal Information Protection and Electronic Documents Act (PIPEDA), substantially similar private sector privacy legislation and public sector and health sector privacy legislation in many provinces. Privacy regulators have also published significant guidance interpreting privacy legislation. Some industries, like the investment industry, have their own

McMillan LLP

Failing to maintain adequate data breach preparedness and response standards can result in potentially significant regulatory penalties, the defence of costly litigation and damages to affected individuals.

specific guidance about privacy and data protection too. Courts in some provinces have begun to recognise and award damages in connection with common law privacy torts, such as intrusion upon seclusion and public disclosure of private facts. Data subjects are increasingly commencing individual actions or class actions against organisations following a data breach, alleging breaches of privacy and related claims. Finally, reputational risks must also be considered, particularly considering mandatory breach reporting and notification in certain circumstances. Further, the results of privacy regulators' investigations into non-compliance with privacy laws may be public, which can contribute to a loss of public confidence if the regulators' findings are unfavourable.

Q. What penalties might arise for a company that breaches or violates data or privacy laws in Canada?

A. Currently, most instances of non-compliance with Canadian privacy laws are addressed through non-binding recommendations following an investigation by one or more privacy regulators. However, regulators can

issue fines in certain circumstances, such as when a business fails to abide by applicable statutory breach reporting obligations. The federal privacy regulator can also refer certain offences to Canada's Attorney General for prosecution. Canada's Competition Bureau has indicated that it may levy significant fines for false or misleading advertising in connection with untruthful or misleading privacy-related representations. This underscores the importance of regularly updating external-facing privacy policies and other privacy documentation to ensure they are complete and accurate.

Q. What insights can we draw from recent data breach cases? What impact have these events had on the data protection landscape?

A. Threat actors are becoming increasingly effective in identifying and exploiting gaps in businesses' security safeguards. At the same time, in part due to the recognition of the advancing sophistication of threat actors, some Canadian privacy regulators and courts have expressed sympathy for businesses that have implemented reasonable preventative measures pre-breach and have taken appropriate steps to minimise any harm to affected individuals post-breach. Companies should continually review and improve their internal data breach prevention and response plans to minimise the likelihood of and negative fallout from a breach. Failing to maintain adequate data breach preparedness and response standards can result in potentially significant regulatory penalties, the defence of costly litigation and damages to affected individuals.

Q. In your experience, what steps should a company take to prepare for a potential data breach, such as developing response plans and understanding notification requirements?

A. Companies must proactively consider the legal, technological and communications needs that flow from a data breach to establish a practical response plan that minimises the potential impact of a breach. Such forethought is critical to a business' ability to swiftly identify and terminate a threat actor's access to its systems and servers, comply with any applicable legal requirements, and establish an effective and controlled

strategy to communicate the breach to regulators, law enforcement, affected individuals and any other relevant stakeholders. From a legal perspective, it is critical to understand the various laws and regulatory guidance that may apply to a company's data processing and breach response requirements. For example, a business that processes personal information about individuals located in different legal jurisdictions may be subject to various Canadian and international privacy laws with differing reporting or notification requirements. It is also important for a company to have strong relationships with qualified privacy counsel in all relevant jurisdictions to quickly coordinate an international breach response strategy as needed. Businesses should also consider maintaining, or requiring their service providers to maintain, cyber risk insurance coverage to help manage legal and other professional costs associated with responding to a data breach.

Q. What can companies do to manage internal risks and threats, such as rogue employees?

A. Companies may implement acceptable use and other policies governing the handling of personal information and the use of information technology resources. PIPEDA requires businesses to train staff regarding their privacy policies and practices. Training should be role-specific and occur both during onboarding and at regular intervals throughout employment, including when there are material changes to policies and practices. Employees should only have access to the personal information needed to perform their duties. Access credentials should be promptly updated or decommissioned and purged when an employee changes roles or departs. Where permitted by applicable law, businesses can also consider implementing access logging and periodic reviews of those logs to spot anomalies. Finally, employees who handle or have access to personal information should generally be subject to appropriate confidentiality and non-disclosure terms, where permitted by law. Oversight is key to ensuring the effectiveness of preventative measures. Employees who fail to meet their obligations with respect to handling personal information should be

subject to disciplinary action in accordance with applicable laws.

Q. Going forward, how important will it be for companies to remain focused on data protection efforts, continually enhancing their controls and risk management processes?

A. It is critical that companies continually review and improve their security safeguards, data breach preparedness and risk management processes. Threat actors continue to identify and exploit gaps in security safeguards and there are no indications that this trend will slow down. Breaches of personal information can potentially undermine hard-earned consumer trust and loyalty. Likewise, the loss of proprietary business information can destroy competitive advantage. To minimise negative reputational, operational and legal risks, data breach prevention and mitigation must become a primary focus for any business that handles sensitive data assets. The potential forthcoming updates to Canada's privacy laws, including the imposition of significant fines for non-compliance, will only increase breach-related risks. Organisations should review their existing privacy compliance programmes, including breach prevention and response measures, to determine whether they are well-positioned to adapt if and when any statutory changes occur.❑

McMillan LLP

www.mcmillan.ca

MCMILLAN is a leading business law firm serving public, private and not-for-profit clients across key industries in Canada, the United States and internationally. With recognised expertise and acknowledged leadership in major business sectors, we provide solutions-oriented legal advice through our offices in Vancouver, Calgary, Toronto, Ottawa, Montréal and Hong Kong. Our firm values – respect, teamwork, commitment, client service and professional excellence – are at the heart of McMillan's commitment to serve our clients, our local communities and the legal profession.

KRISTEN PENNINGTON Partner
+1 (416) 865 7943
kristen.pennington@mcmillan.ca

MITCH KOCZERGINSKI Associate
+1 (416) 865 7262
mitch.koczerginski@mcmillan.ca

LYNDSAY WASSER Partner
+1 (416) 865 7083
lyndsay.wasser@mcmillan.ca

GRACE SHAW Associate
+1 (236) 826 3064
grace.shaw@mcmillan.ca