Canadian Privacy Law Review

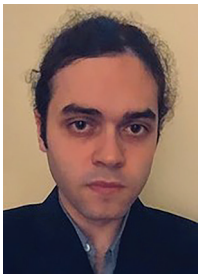
VOLUME 19, NUMBER 3 Cited as (2022), 19 C.P.L.R. FEBRUARY 2022

• FEDERAL PRIVACY COMMISSIONER RELEASES MORE GUIDANCE FOR VIDEO TELECONFERENCING COMPANIES •

Kristen Pennington, Partner, and Kamal Azmy, Articling Student, McMillan LLP

• In This Issue •

Kristen Pennington



Kamal Azmy

In July 2020, the Office of the Privacy Commissioner of Canada (the "OPC"), along with its international counterparts, sent a letter[1] to five of the largest video teleconferencing companies ("VTCs") inviting them to discuss how they address key privacy risks associated with video teleconferencing.

Based on the responses from some of the VTCs, the OPC recently shared[2] some good practices and areas for improvement within the video teleconferencing industry.

SECURITY

The OPC endorsed VTCs adopting a mix of vulnerability testing measures, including:

- "bug bounty" programs, through which VTCs would compensate users who identify and report security exploits;
- independent audits of VTCs' privacy and security measures; and
- simulated cyber-attacks.

CANADIAN PRIVACY LAW REVIEW

Canadian Privacy Law Review is published monthly by LexisNexis Canada Inc., 111 Gordon Baker Road, Suite 900, Toronto ON M2H 3R1 by subscription only.

ISBN 0-433-44419-3 (print) ISSN 1708-5446
ISBN 0-433-44652-8 (PDF) ISSN 1708-5454
ISBN 0-433-44420-7 (print & PDF)

Subscription rates: $395.00 per year (print or PDF)
$600.00 per year (print & PDF)

Please address all editorial inquiries to:

General Editor
Professor Michael A. Geist
Canada Research Chair in Internet and E-Commerce Law
University of Ottawa, Faculty of Law
E-mail: mgeist@uottawa.ca

LexisNexis Canada Inc.
Tel. (905) 479-2665
Fax (905) 479-2826
E-mail: cplr@lexisnexis.ca
Web site: www.lexisnexis.ca

VTCs are also encouraged to implement pre-employment checks (subject to applicable employment and privacy laws), regular employee training programs, and vetting and auditing procedures for third party data processors to ensure compliance with applicable data protection obligations.

PRIVACY-BY-DESIGN AND DEFAULT

VTCs are encouraged not to treat privacy as an afterthought, and instead to proactively consider the privacy implications of new features. The OPC also recommended making standard user settings the most privacy-protecting options, for example by configuring meeting passwords and waiting rooms to be automatically enabled, and cameras and microphones to be disabled, by default.

KNOW YOUR AUDIENCE

Recognizing the increased use of video teleconferencing in privacy-sensitive contexts such as education and healthcare, the OPC has highlighted industry-specific best practices, such as teacher-controlled access to school meetings and secure screen sharing of health documents.

The OPC also recommends that VTCs create tailored guidance about the privacy features of their platforms for specific groups of users and use cases, to help individuals select the privacy settings and features most appropriate for them.

TRANSPARENCY

The OPC endorses a layered approach to alerting users to the collection and use of their personal information, including through the use of notifications both before and during a video call.

The OPC has also stressed the importance of transparency when users' information is shared with third parties and requires that users be notified about what is shared, with whom it is shared and the reasons for doing so. Strategies in this respect could include up-to-date privacy notices setting out this information, as well as advance notification periods for the use of new third party processors.

END-USER CONTROL

The OPC recommends the implementation of several features to allow end users to exert control over the collection and use of their personal information, including allowing users to enable virtual and blurred backgrounds, requiring an individual's consent prior to a host activating their microphone or webcam, and the inclusion of tools for users to report inappropriate conduct during a video call.

ENCRYPTION

The OPC recommends that VTCs:

- make end-to-end encryption an option for all users;
- clearly communicate the differences between end-to-end and standard encryption;
- clearly present meeting controls that allow users to select and see the type of encryption used in a meeting; and
- enable end-to-end encryption by default in privacy-sensitive contexts such as tele-health.

SECONDARY USES OF PERSONAL INFORMATION

Where personal information is used for purposes other than to provide functionality to the features of a video teleconferencing service, the OPC recommends that VTCs make this clear with plain language, direct and proactive messaging, explaining what personal information will be used for secondary purposes and why.

If these secondary purposes include targeted advertising or tracking, the OPC recommends that VTCs only engage in such practices if users have opted-in.

STORAGE OF PERSONAL INFORMATION

The OPC recommends that VTCs clearly communicate to users where their personal information will be stored and, where possible, give users choice over where their personal information is stored. In any event, VTCs should take appropriate steps to ensure that personal information is adequately protected wherever it is stored.

IMPLICATIONS FOR BUSINESSES

The implications for VTCs are clear: consider implementing these recommendations of the OPC or risk adverse findings in the event of a privacy complaint or investigation initiated by the OPC.

However, many of the points raised by the OPC in this guidance echo existing statutory obligations, regulatory guidance and/or past investigation findings by the OPC which apply to a wide variety of organizations who collect, use or disclose personal information in the course of their commercial activities. This guidance therefore serves as a good reminder to consider privacy law implications early in the design phase of a new product or service and to be vigilant for ways to improve privacy and data protection practices throughout the lifecycle of that product or service.

Moreover, organizations governed by Canadian privacy laws should keep in mind that they are generally accountable for the processing of personal information by their service providers. This includes conducting appropriate due diligence to assess vendors' data handling practices and compliance with Canadian privacy laws. Organizations are advised to carefully consider the privacy practices and features of any video teleconferencing platforms used, including the points raised by the OPC in this guidance. Implementing appropriate policies and training for employees who use video teleconferencing platforms to perform their duties is also recommended to prevent data breaches and other privacy mishaps.

A CATIONARY NOTE

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.

[***Kristen Pennington*** *is a Partner in the Privacy & Data Protection Group of McMillan LLP. Kristen counsels clients on the privacy law implications of new products, technologies, initiatives and corporate transactions. She also helps organizations develop privacy compliance programs and drafts privacy policies and privacy and data protection terms in an array of commercial agreements.*

Kamal Azmy *is an articling student in McMillan LLP's Toronto office. Kamal is a recent graduate of the University of Toronto's Faculty of Law, and before that graduated with a business degree from Memorial University of Newfoundland.*]

---

1 Grace Shaw, "Global Privacy Authorities Remind Video Teleconferencing Companies of Privacy Expectations" (29 July 2020), online: McMillan LLP https://mcmillan.ca/insights/global-privacy-authorities-remind-video-teleconferencing-companies-of-privacy-expectations/.

2 "Observations following the joint statement on global privacy expectations of video teleconferencing companies" (27 October 2021), online: Office of the Privacy Commissioner of Canada https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/vtc_211027/.

• SETTING NEW STANDARDS FOR CYBER RESILIENCE: OSFI'S DRAFT GUIDELINE ON TECHNOLOGY AND CYBER RISK MANAGEMENT •

Koker Christensen, Partner, Alex Cameron, Partner, Christopher Ferguson, Partner, Justin P'ng, Associate, and Jasmeen Kabuli, Articling Student, Fasken Martineau DuMoulin LLP

Koker Christensen

Alex Cameron

Christopher Ferguson

Justin P'ng

Jasmeen Kabuli

This *article was reprinted with the permission of Fasken. Fasken is one of the world's leading international business law and litigation firms. For more information about Fasken's Privacy and*

Cybersecurity Group and Financial Services Group, please visit www.fasken.com.

On November 9, 2021, the Office of the Superintendent of Financial Institutions Canada (OSFI) published Draft Guideline B-13: Technology and Cyber Risk Management ("Draft Guideline"), which outlines OSFI's expectations for federally regulated financial institutions (FRFIs) regarding technology and cyber risk management. The Draft Guideline would apply to all FRFIs, including banks and insurance companies, with the stated objective of helping FRFIs develop "greater resilience to technology and cyber risks". Effective November 9, 2021, OSFI is also conducting a three-month public consultation on the Draft Guideline to engage stakeholders in its development and is inviting public comments until February 9, 2022.

MEANING OF TECHNOLOGY RISK AND CYBER RISK

The Draft Guideline uses materially similar definitions for "technology risks" and "cyber risks":

- A technology risk is the "risk arising from the inadequacy, disruption, failure, loss or malicious use of information technology systems, infrastructure, people or processes that enable and support business needs and can result in financial loss".
- A cyber risk is the "risk of financial loss, operational disruption or reputational damage from the unauthorized access, malicious and non-malicious use, failure, disclosure, disruption, modification or destruction of an institution's information technology systems and/or the data contained therein".

Although these definitions both capture risks to information technology systems and the potential for financial loss, a key distinguishing feature is that cyber risks also include risks to the data hosted in information technology systems as distinct from the technology itself, whereas technology risks also include risks to other infrastructure, people, and processes. Further, cyber risks encompass a broader range of potential harms, including operational disruption and reputational damage.

SUMMARY OF OSFI'S EXPECTATIONS FOR TECHNOLOGY AND CYBER RISK MANAGEMENT

The Draft Guideline is organized into five domains: Governance and Risk Management, Technology Operations, Cyber Security, Third-Party Provider Technology and Cyber Risk, and Technology Resilience. Each domain sets out OSFI's expectations, the key components of sound technology and cyber risk management, the desired risk management outcome, and guiding principles, which are summarized in the table below. FRFIs will be evaluated on these expectations commensurate with their size, the nature, scope, complexity of their operations, and their risk profiles:

Domain 1 Governance and Risk Management	***Expectations:*** Sets OSFI's expectations on formal accountability, leadership, organizational structure and framework used to support risk management and oversight of technology and cyber security. ***Desired Outcome:*** Technology and cyber risks are governed through clear accountabilities and structures, and comprehensive strategies and frameworks. ***Principles (1 to 3):*** 1. **Accountability and Organization Structure:** Senior Management should assign responsibility for managing technology and cyber risks to senior officers, and also ensure an appropriate organizational structure and adequate resourcing are in place for managing technology and cyber risks across the FRFI. 2. **Technology and Cyber Strategy:** The FRFI should define, document, approve and implement a strategic technology and cyber plan(s) that aligns to the FRFI's business strategy while setting goals and objectives that are measurable and evolve with changes in the FRFI's technology and cyber environment. 3. **Technology and Cyber Risk Management Framework:** The FRFI should establish a technology and cyber risk management framework (RMF). The framework should set out a risk appetite for technology and cyber risks, and define what processes and requirements the FRFI utilizes to identify, assess, manage, monitor and report on technology and cyber risks.

Domain 2 Technology Operations	***Expectations:*** Sets OSFI's expectations on management and oversight of risks related to the design, implementation and management of technology assets and services. ***Desired Outcome:*** A technology environment that is stable, scalable and resilient. The environment is kept current and supported by robust and sustainable technology operating processes. ***Principles (4 to 11):*** 4. **Technology Architecture:** The FRFI should implement a technology architecture framework, with supporting processes to ensure solutions are built in line with business, technology and security requirements. 5. **Technology Asset Management:** The FRFI should maintain an updated inventory of all technology assets supporting business processes or functions. The FRFI's asset management process should address classification of assets to facilitate risk identification and assessment, record configurations to ensure asset integrity, provide for the safe disposal of assets at the end of their life cycle, and monitor and manage technology currency. 6. **Technology Project Management:** Effective processes are in place to govern and manage technology projects, from initiation to closure, to ensure that project outcomes are aligned with business objectives and are achieved within the FRFI's risk appetite. 7. **System Development Life Cycle:** The FRFI should implement a System Development Life Cycle (SDLC) framework for the secure development, acquisition and maintenance of technology systems that perform as expected in support of business objectives.
	8. **Change and Release Management:** The FRFI should establish and implement a technology change and release management process and supporting documentation to ensure changes to technology assets are documented, assessed, tested, approved, implemented and verified in a controlled manner that ensures minimal disruption to the production environment. 9. **Patch Management:** The FRFI should implement patch management processes to ensure controlled and timely application of patches across its technology environment to address vulnerabilities and flaws. 10. **Incident and Problem Management:** The FRFI should effectively detect, log, manage, resolve, monitor and report on technology incidents and minimize their impacts. 11. **Technology Service Measurement and Monitoring:** The FRFI should develop service and capacity standards, and processes to monitor operational management of technology, ensuring business needs are met.
Domain 3 Cyber Security	***Expectations:*** Sets OSFI's expectations on management and oversight of cyber risk. ***Desired Outcome:*** A secure technology posture that maintains the confidentiality, integrity and availability of the FRFI's technology assets. ***Principles (12 to 15):*** 12. **Identify:** The FRFI should maintain a range of practices, capabilities, processes and tools to identify and assess cyber security for weaknesses that could be exploited by external and insider threat actors.
	13. **Defend:** The FRFI should design, implement and maintain multi-layer, preventive cyber security controls and measures to safeguard its technology assets. 14. **Detect:** The FRFI designs, implements and maintains continuous security detection capabilities to enable monitoring, alerting, and enable forensic cyber security incident investigations. 15. **Respond, Recover and Learn:** The FRFI should triage, respond to, contain, recover and learn from cyber security incidents impacting its technology assets, including incidents originating at third-party providers.
Domain 4 Third-Party Provider Technology and Cyber Risk	***Expectations:*** Expands on OSFI's existing guidance for outsourcing and third-party risk, and sets expectations for FRFIs that engage with third-party providers to obtain technology and cyber services that give rise to cyber and/or technology risk. ***Desired Outcome:*** Reliable and secure technology and cyber operations from third-party providers. ***Principles (16):*** 16. **General:** The FRFI should ensure that effective controls and processes are implemented to identify, assess, manage, monitor, report and mitigate technology and cyber risks throughout the TPP's life cycle, from due diligence to termination/exit.
Domain 5 Technology Resilience	***Expectations:*** Sets OSFI's expectations on the capabilities to deliver technology services through operational disruption. ***Desired Outcome:*** Technology services are delivered, as expected, through disruption. ***Principles (17):*** 17. Disaster Recovery: The FRFI should establish and maintain an Enterprise Disaster Recovery Framework (EDRF) to support its ability to deliver technology services through disruption and operate within its risk tolerance.

The Draft Guideline acknowledges that technology and cyber security best practices are fluid and dynamic, and encourages FRFIs to also consult other OSFI guidance, tools and supervisory communications, along with other applicable guidance from relevant authorities, particularly the following:

- OSFI Guideline E-21: Operational Risk Management (summarized in our previous bulletin, "OSFI Releases Final Operational Risk Management Guideline");
- OSFI Guideline B-10: Outsourcing (note that OSFI is undertaking a review of Guideline B-10);

- OSFI Cyber Security Self-Assessment Tool (summarized in our previous bulletin, "Updated OSFI Advisory: Technology and Cyber Security Incident Reporting");
- OSFI Technology and Cyber Security Incident Reporting Advisory (summarized in our previous bulletin, "Updated OSFI Advisory: Technology and Cyber Security Incident Reporting");
- Alerts, advisories and other communications issued by the Canadian Centre for Cyber Security; and,
- Recognized frameworks and standards for technology operations and information security.

PUBLIC CONSULTATION

OSFI's three-month public consultation is intended to reflect continued stakeholder engagement and transparency on the Draft Guideline, and to assist OSFI in striking a balance between its prudential objectives and facilitating the ability of financial institutions to compete. Public comments are particularly welcomed by OSFI on:

- the clarity of OSFI's expectations as set out in the Draft Guideline;
- the application of these expectations, commensurate with the institution's size, nature, scope, and complexity of operations;
- the balance between principles and prescriptiveness in OSFI's expectations; and
- other suggestions that contribute to OSFI's mandate to protect depositors and policyholders, and maintain public confidence in the Canadian financial system, while also allowing institutions to compete and take reasonable risks.

Comments can be submitted to Tech.Cyber@osfi-bsif.gc.ca by February 9, 2022. OSFI is also planning an information session for financial institutions within the coming weeks to provide an overview of the Draft Guideline and an opportunity for questions.

TAKEAWAYS FOR FRFIS AND THIRD-PARTY PROVIDERS

The publication of the Draft Guideline is pursuant to OSFI's Near-Term Plan of Prudential Policy published on May 6, 2021 ("Near-Term Plan"), which expressly committed OSFI to developing OSFI's expectations on technology and cyber risk management in Q4 of 2021. As indicated in the Near-Term Plan and Draft Guideline, OSFI's next objective is to update Guideline B-10: Outsourcing of Business Activities, Functions and Processes in Q1 of 2022, and to expand its scope of third-party risk management beyond outsourcing. Accordingly, FRFIs and their third-party providers can expect additional significant regulatory developments and should begin to strategically prepare for the potential impact on their operations.

FRFIs should review their technology and cyber risk management frameworks and third party service agreements to prepare for OSFI's new focus on these issues. Although the Draft Guideline is subject to further development after the public consultation, FRFIs should expect that its key themes will generally be maintained, and that its final expectations will go beyond making additional investments in information technology and security. While these are of course critical to any technology and cyber risk management framework, FRFIs may also need to revisit their practices with respect to governance, risk accountability, asset management, and relationships with third-party providers. For their part, third-party providers that provide information technology and other services to FRFIs may also need to revisit their Canadian financial industry templates and related practices to account for these new regulatory developments.

[***Koker Christensen*** *is Co-Leader of the firm's Financial Services Group. He advises businesses in the financial services sector, including insurers, banks, trust companies, credit unions, payments businesses, fintechs and insurtechs. His areas of expertise include M&A, reinsurance transactions, regulatory matters, anti-money laundering and corporate governance. He also advises financial institutions on incorporation and licensing. Koker can be reached by email at kchristensen@fasken.com.*

Alex Cameron *is co-leader of the firm's Privacy and Cybersecurity Group. Clients from all sectors, including numerous Fortune 100 and 500 companies,*

consistently turn to Alex for his recognized leading expertise in privacy, cybersecurity and related matters. Clients work closely with Alex to achieve business objectives through the innovative use of personal information, while ensuring compliance and managing risk. Alex can be reached by email at acameron@fasken.com.

***Christopher Ferguson's** practice is focused on technology, privacy, intellectual property, and regulatory matters. Christopher regularly advises on IT and technology matters, including negotiating and drafting services, outsourcing, and license agreements, along with legal and regulatory developments in the technology sector. Christopher can be reached by email at cferguson@fasken.com.*

***Justin P'ng** is an Associate in Fasken's Privacy and Cybersecurity Group. He advises private and public sector organizations on various privacy matters, including privacy policies and procedures, data protection, privacy impact assessments, access to information requests, employee privacy, incident response planning, and compliance with privacy laws. Justin can be reached by email at jpng@fasken.com.*

***Jasmeen Kabuli** graduated from Osgoode Hall Law School. Prior to law school, she obtained an Honours Bachelor of Commerce with specialization in Finance from York University where she graduated on the Dean's Honour Roll. Jasmeen can be reached by email at jkabuli@fasken.com.*]

• BRITISH COLUMBIA MAKES SIGNIFICANT CHANGES TO FIPPA INCLUDING NEW DATA SOVEREIGNTY RULES •

David Crane, Partner, Jade Buchanan, Partner, Kelsey Franks, Associate, and Curtis Chance, Associate, McCarthy Tétrault LLP

David Crane

Jade Buchanan

Kelsey Franks

Curtis Chance

On November 25, 2021, the Legislative Assembly of British Columbia passed Bill 22 (the "Bill")[1] to amend the *Freedom of Information and Protection of Privacy Act* ("FIPPA"),[2] which governs how public bodies in British Columbia collect, use, store and disclose personal information. When presenting the Bill in British Columbia's Legislative Assembly, Minister of Citizens' Services Lisa Beare stated that the Bill responds to the need for safe and convenient online services and aims to enhance privacy protection and ensure that government can provide a level of service that keeps pace with new technology.

The amendments significantly change privacy regulation under FIPPA. Notably, the Bill:

1. eliminates the prohibition on disclosing, storing and allowing access to personal information outside of Canada;
2. introduces a requirement that public bodies develop a privacy management program;
3. introduces a requirement that public bodies that experience a privacy breach notify affected individuals and the British Columbia Information and Privacy Commissioner (the "Commissioner") where a privacy breach could

be reasonably expected to result in significant harm; and

4. introduces new privacy offences, including where a person willfully collects, uses or discloses personal information except as authorized by FIPPA.

This blog post will explore each of these amendments included in the Bill in greater detail. The amendments about data sovereignty and privacy offences are now in force. We do not discuss the data-linking and freedom of information-related amendments that are also in the Bill.

DATA SOVEREIGNTY REQUIREMENTS

Previously, under sections 30.1 and 33.1 of FIPPA, public bodies were not permitted to disclose, store or allow access to personal information outside of Canada, except in narrow and defined circumstances. Taken together, the general rule was that public bodies could only engage service providers, such as cloud hosting service providers, that stored personal information in Canada, or obtain consent from each individual whose information the public body collected, to store or allow access to such personal information outside of Canada. These restrictions, combined with the fact that many service providers do not have a physical presence in Canada, limited the ability of public bodies in British Columbia to access a broader market of service providers.

The Bill repeals the prohibition on disclosing, storing and allowing access to personal information outside of Canada. Instead, a public body may disclose personal information outside of Canada if the disclosure is in accordance with the regulations.[3] One applicable regulation has been published to date: on November 26, 2021, the Minister of Citizens' Services published the *Personal Information Disclosure for Storage Outside of Canada Regulation* (the "Regulation"),[4] which requires the head of a public body to make a privacy impact assessment ("PIA") in accordance with FIPPA with respect to each of the public body's programs, projects and systems in which sensitive personal information is disclosed to be stored outside of Canada. Notably, this requirement does not apply to programs, projects and systems in place at the time the regulation came into force.

Independently of the amendments to section 33.1, amendments to section 33(2)(u) permit disclosure of personal information outside of Canada for processing if the processing done outside of Canada is temporary. The implications of the amendments to section 33(2)(u) and their interaction with the amendments to section 33.1 remain to be seen.

These data sovereignty amendments are consistent with the spirit of the temporary relaxation of data sovereignty requirements introduced on March 26, 2020, when the Minister of Citizens' Services issued Ministerial Order M085 (the "Order")[5]. The Order temporarily permitted public bodies to disclose personal information outside of Canada for limited purposes through third party tools and applications. It was designed to allow public bodies to deliver digital services throughout the COVID-19 pandemic. The Order is set to expire on December 31, 2021.[6]

The amendments to the data sovereignty requirements were met with opposition from the Commissioner, who wrote: "What is exceedingly troubling however, is that government now proposes to allow public bodies to send British Columbians' personal information outside Canada without explaining how they will properly protect it."[7] However, it is notable that FIPPA still requires public bodies to protect personal information in their control or custody by making reasonable security arrangements against risks such as unauthorized collection, use, disclosure or disposal.[8] Accordingly, while the changes in the Bill provide public bodies with more flexibility in where personal information is stored and accessed from, public bodies are still required to ensure personal information is protected through reasonable security measures, which could include contractual and technical solutions such as encryption. The extent and type of security measures may also be informed by the PIA, meaning there will be a consideration of the security implications of transferring personal information outside of Canada.

It remains to be seen if the Regulation adequately address the Commissioner's concerns. He has not, as of December 15, 2021, commented on the Regulation and whether it resolves the concerns he raised prior to the publication of the Regulation.

The Bill also brings FIPPA into closer alignment with public sector privacy legislation from other provinces. Currently, in all provinces except Newfoundland and Labrador,[9] Nova Scotia,[10] and Quebec,[11] there are no additional restrictions on provincial public bodies disclosing, storing or allowing access to personal information outside of Canada or the applicable province.

PRIVACY MANAGEMENT REQUIREMENTS

The Bill proposes a new requirement for public bodies to develop a privacy management program. Under the proposed section 36.2, the privacy management program must be prepared in accordance with the directions of the Minister of Citizens' Services, yet to be released.[12]

Commenting on this addition the Commissioner stated: "I welcome the new requirements relating to privacy impact assessments, the new privacy breach notification rules, and the duty for public bodies to have privacy management programs."[13] The Commissioner already provides guidance to public bodies on privacy management programs, in its "Accountable Privacy Management in BC's Public Sector" publication,[14] which may inform the requirements under FIPPA.

PRIVACY BREACH NOTIFICATION REQUIREMENTS

The Bill also proposes a new privacy breach notification requirement on public bodies. Under the proposed section 36.3, if personal information in the custody of or under the control of a public body is stolen or lost, or collected, used or disclosed without being authorized by FIPPA, the head of the public body must notify the affected individual without unreasonable delay if the privacy breach could reasonably be expected to result in significant harm to the individual. The public body is also required to notify the Commissioner in such circumstance.

The significant harm contemplated by the section includes identity theft, bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, negative impact on a credit record, or damage to or loss of property.[15] Specific exceptions are carved out of the notification requirement if notifying the individual of the privacy breach could reasonably be expected to result in immediate and grave harm to the individual or another individual's safety, physical health or mental health.

As noted above, the Commissioner supports the proposed privacy breach notification requirements; however, the Commissioner also suggested that an additional exception to the requirement be made where disclosure of the breach could compromise a criminal investigation. He also stated that such an exception would be "consistent with similar provisions elsewhere."[16] Currently, Saskatchewan, Ontario, Newfoundland and Labrador, Yukon, Northwest Territories, and Nunavut have similar provisions that require public bodies to notify commissioners and affected individuals when personal information is stolen or lost, or collected, used or disclosed without authorization,[17] although the exact wording, timing of notification, and threshold for harm vary across the jurisdictions. The Bill did not include this exception when passed.

PRIVACY OFFENCES

The Bill also introduces Part 5.1 to address offences under FIPPA, including the introduction addition of "snooping offences". The willful collection, use, disclosure or failure to notify the head of the public body of an unauthorized disclosure of personal information, except as authorized under FIPPA, is now an offence. This offence expressly applies to service providers and employees or associates of

service providers, but also applies to other individuals. Notably, the Bill states that service providers themselves commit an offence if their employee or associate commits a snooping offence.

The Commissioner welcomed the creation of snooping offences stating that such offences "do occur and must be deterred or punished appropriately"[18] but expressed concern that the amendments do not go far enough. Specifically, he suggested that the provision should explicitly make "viewing" and "accessing" personal information, except as authorized under FIPPA, an offence as well, submitting that these additions would make it entirely clear that "an individual's mere observation of personal information is a collection of that information" and therefore, an offence.[19] The Bill also did not include these additions when passed.

Other jurisdictions in Canada already have introduced snooping offences into their relevant public sector privacy legislation. Each of Alberta, Saskatchewan, Newfoundland and Labrador, Prince Edward Island, Northwest Territories, Yukon, and Nunavut prohibit the collection, use or unauthorized disclosure of personal information, except as authorized under the relevant statute.[20]

CONCLUSION

The amendments to FIPPA in the Bill signal that the Government of British Columbia recognizes that the existing data sovereignty requirements are too inflexible for public bodies seeking access to a broad global market of potential service providers, and that there are opportunities for enhancing privacy protection through the introduction of new privacy offences, privacy breach notification and privacy management program requirements.

[***David Crane*** *is a Chambers-ranked information technology partner in McCarthy Tétrault's Vancouver office. For over 15 years, David has been assisting clients in a wide range of sectors with their complex and strategic technology-related transactions. With a deep understanding of not only the legal issues, but also the business and technological issues that arise from established and emerging technologies, he brings a practical, solution-oriented approach to getting deals done efficiently and effectively.*

Jade Buchanan *is a partner in McCarthy Tétrault's Vancouver office and part of our Cyber/Data and Technology Groups. One the Global Data Review's leading 40 Under 40 data lawyers in the world for 2021, Jade has worked on some of the largest cybersecurity incidents in Canadian history and dozens of other incidents, including data breaches and ransomware attacks. Beyond experience with Canada's and British Columbia's private sector privacy legislation (PIPEDA, CASL and PIPA), Jade has extensive experience advising on British Columbia's public sector legislation (the Freedom of Information and Protection of Privacy Act) for public bodies and their service providers. Jade is also a Certified Information Privacy Professional (Canada).*

Kelsey Franks *is an associate in McCarthy Tétrault's Cyber/Data and Technology Groups in the Vancouver office. Kelsey is building a practice in information technology and privacy law and has particular experience with public-sector technology projects and privacy compliance. In law school Kelsey was an executive editor of the McGill Law Journal.*

Curtis Chance *is an associate in the business law group of McCarthy Tétrault's Vancouver office. Curtis is building a practice that includes privacy and information technology law. Curtis clerked for two justices at the British Columbia Court of Appeal.*]

---

1 Bill 22, *Freedom of Information and Protection of Privacy Amendment Act, 2021*, 2nd Sess, 42nd Parl, British Columbia, 2021, online: https://www.leg.bc.ca/parliamentary-business/legislation-debates-proceedings/42nd-parliament/2nd-session/bills/third-reading/gov22-3.

2 *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165.

3 *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165, s. 33.1.

[4] Province of British Columbia, Ministerial Order No. M462, online: https://www.bclaws.gov.bc.ca/civix/document/id/mo/mo/m0462_2021.

[5] Province of British Columbia, Ministerial Order No. M085, online: https://www.bclaws.gov.bc.ca/civix/document/id/mo/mo/m0085_2020.

[6] Province of British Columbia, Ministerial Order No. M192, online: https://www.bclaws.gov.bc.ca/civix/document/id/mo/mo/m0192_2021.

[7] "Statement from BC Information and Privacy Commissioner regarding proposed amendments to the *Freedom of Information and Protection of Privacy Act*" (18 October 2021), online: Office of the Information & Privacy Commissioner for British Columbia https://www.oipc.bc.ca/news-releases/3591.

[8] *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165, s. 30.

[9] *Personal Health Information Act*, S.N.L. 2008, c. P-7.01, s. 47.

[10] *Personal Information International Disclosure Protection Act, 2006*, S.N.S. 2006, c. 3.

[11] Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, CQLR C. A-2.1, s. 70.1.

[12] "Progress of Bills", 2nd Sess, 42nd Parl, 2021, online: https://www.leg.bc.ca/parliamentary-business/legislation-debates-proceedings/42nd-parliament/2nd-session/bills/progress-of-bills.

[13] Letter from Michael McEvoy, Information and Privacy Commissioner for British Columbia to Minister Lisa Beare, Minister of Citizens' Services (20 October 2021), online: https://www.oipc.bc.ca/public-comments/3592.

[14] "Accountable Privacy Management in BC's Public Sector", online: Office of the Information & Privacy Commissioner for British Columbia https://www.oipc.bc.ca/guidance-documents/1545.

[15] "Progress of Bills", 2nd Sess, 42nd Parl, 2021, online: https://www.leg.bc.ca/parliamentary-business/legislation-debates-proceedings/42nd-parliament/2nd-session/bills/progress-of-bills. These significant harms are substantially similar to those listed in the federal government's *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5.

[16] Letter from Michael McEvoy, Information and Privacy Commissioner for British Columbia to Minister Lisa Beare, Minister of Citizens' Services (20 October 2021), online: https://www.oipc.bc.ca/public-comments/3592.

[17] *Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. F-22.01, s. 29.1; *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F.31, s. 49.11; *Access to Information and Protection of Privacy Act, 2015*, S.N.L. 2015, c. A-1.2, s. 64; *Access to Information and Protection of Privacy Act*, S.Y. 2018, c. 9, amended by S.Y. 2019, c. 15, s. 32; *Access to Information and Protection of Privacy Act*, S.N.W.T. 1994, c. 20, cc. 49.7 and 49.10; Consolidation of *Access to Information and Protection of Privacy Act*, S.N.W.T. 1994, c. 20, ss. 49.7 – 49.10.

[18] Letter from Michael McEvoy, Information and Privacy Commissioner for British Columbia to Minister Lisa Beare, Minister of Citizens' Services (20 October 2021), online: https://www.oipc.bc.ca/public-comments/3592.

[19] Letter from Michael McEvoy, Information and Privacy Commissioner for British Columbia to Minister Lisa Beare, Minister of Citizens' Services (20 October 2021), online: https://www.oipc.bc.ca/public-comments/3592.

[20] *Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c. F-25, s. 92; *Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. F-22.01, s. 68; *Access to Information and Protection of Privacy Act, 2015*, S.N.L. 2015, c. A-1.2, s. 115; *Freedom of Information and Protection of Privacy Act*, RS.P.E.I. 1988, c. F-15.01, s. 75; *Access to Information and Protection of Privacy Act*, S.N.W.T. 1994, c. 20, s. 59; *Access to Information and Protection of Privacy Act*, S.Y. 2018, c. 9, amended by S.Y. 2019, c. 15, s. 121; Consolidation of *Access to Information and Protection of Privacy Act*, S.N.W.T. 1994, c. 20, s. 59.

• RISKS OF ANONYMIZED AND AGGREGATED DATA •

Robert C. Piasentin, Partner, and Kristen Shaw, Articling Student, McMillan LLP

Robert C. Piasentin

Kristen Shaw

Data drives many business decisions in today's digital economy. How that data is used is facing greater scrutiny, in particular when that data can identify specific individuals. As a result, businesses are seeking alternative ways to use data in a way that, they hope, will allow them to continue to reap the benefits of using such data while also staying on the right side of all applicable privacy requirements. Many businesses, for example, use technology to aggregate data for a number of reasons including making their marketing and product development processes more efficient and effective. Relatedly, companies will often seek to anonymize the data they collect in order to try to avoid the application of privacy requirements. However, simply using anonymized and/or aggregated data does not insulate a business from the risk of privacy violations, it may instead just give a business a false sense of security with respect to that risk. If a business anonymizes and simply aggregates collected data into a group of unidentified data points, how can it be at risk? In this bulletin, we will touch on the risks and considerations that a business should focus on when using such data in its operations.

WHAT DOES IT MEAN TO BE IDENTIFIABLE?

The restrictions on the collection, use, and disclosure of data in privacy laws across the globe are triggered when data can be used to identify a specific person.[1] For example, British Columbia's *Personal Information Protection Act* ("*PIPA*") provides protection for information which falls within the definition of "personal information".[2] Personal information is defined as "information about an identifiable individual" and it is generally thought to include primary identifiers such as one's name, age, address, fingerprints, ethnic origin, and marital status.[3] Canada's federal privacy legislation, the *Personal Information Protection and Electronic Documents Act* ("*PIPEDA*"),[4] applies the same concept regarding personal information.

Risks and Challenges of Anonymization

Anonymization, or de-identification, refers to a process that removes information capable of identifying individuals or their households from collected data.[5] The risk with anonymizing data is that it can often be re-identified – where anonymized data is matched with available information to discover the individual to whom it belongs. However, there are a number of practices that can be used to help reduce the risk of re-identification. For example, statistical "white noise" can be introduced to obscure the connections between data elements, or obfuscation can render data less accessible.[6] Many organizations struggle with finding the right balance of anonymization largely because, while greater anonymization of data affords better privacy protection, the usefulness of that data is correspondingly reduced. The trick is finding an optimal state between the two extremes.[7]

While anonymizing data is a strong start to avoiding violating an individual's privacy, "personal information" is often defined quite broadly such that certain types of data are not truly capable of being anonymized. For example, sensor data collected from passive smart home devices poses particular challenges to traditional methods of anonymization. While voice or video data can be obscured, and digital profiles containing primary identifiers can be segregated or encrypted, the nature of

sensor data makes it challenging to de-identify. Sensor data is a collection of a user's activities where specific personally identifiable elements cannot be easily removed or obscured.[8] As a result, sensor data is more prone to re-identification due to the unique imperfections and irregularities within the sensor.[9] Basically, sensors are susceptible to having slight flaws or differences between them, and those flaws can act like a fingerprint to identify data that comes from a particular device.

The Implications of Aggregate Data

Alongside the risks of anonymization come the risks of such data being used and disclosed in the aggregate. Much of the data collected by smart home devices, wearables, and other Internet of Things ("IoT") technologies is not directly identifiable, but still may be deeply personal, and may create an identifiable profile when aggregated. The purpose for the collection of such data is crucially linked to the function of most IoT devices – to better understand the behaviour, habits, and preferences of the user.[10] The combined mass, however, creates a picture of the user that can lead to identifiable personal information for a specific individual.

Aggregated data, which combines various discrete data points specific to a particular individual, can provide substantial and surprising inferences about private behaviours and habits that an individual never intended to share.[11] These unintended consequences are exacerbated by the developments in AI that allow data processors to extract data trends and relationships that were previously inconceivable by data scientists.[12]

One phenomenon, known as "sensor fusion", will likely become more prominent as the market uptake of IoT devices increases and their presence multiplies within the home. Sensor fusion is where data from two sensing devices can reveal greater information, and perhaps unexpected inferences, when that data is combined.[13] This phenomenon may also mean that a sensor within an IoT device is used for purposes beyond its intended and original use, particularly when used alongside other IoT devices.[14] Sensor fusion raises legitimate concerns regarding whether an individual has provided or can provide informed consent, where unintended uses could not be adequately communicated to the user in advance, and creates risks for those selling and incorporating such technologies in their businesses.

These risks remain even when information is de-identified, largely due to the fact that the distinctive nature of this data makes it relatively easy to identify the individual to whom the data belongs.[15] In fact, the Office of the Privacy Commissioner ("OPC") has been critical of an approach which characterizes technologies which anonymize data at particular points in their use as offering anonymity where identification of an individual, while highly improbable, is not impossible.[16] Further, the Supreme Court of Canada has made it clear that when considering a user's reasonable expectation of privacy, it is not enough to only consider each data point in isolation, but consider what the whole may reveal about the personal habits and choices of the individual behind the data.[17]

CAN YOU FREELY USE ANONYMIZED AND AGGREGATED DATA?

While truly anonymized data, whether in an aggregated form or not, can be freely used and shared, the ability to glean personal information from both anonymized and aggregated data creates risks for using and disclosing such data for commercial purposes because there is always a risk of re-identification. Privacy laws currently rely on the assumption that it is possible to distinguish between what is "personally identifiable information" and anonymized or aggregated data,[18] however this assumption does not entirely absolve a company from risk.

Approximately 99.98% of anonymized data may be capable of re-identification and, as explored above, the risks of re-identification are heightened when data is aggregated.[19] It is currently uncertain whether, and how, Canadian privacy legislation may consider these risks. There is a global trend towards incorporating re-identifiable data under privacy protections. The GDPR, for example, considers "pseudonymous data", which is data that does not contain direct identifiers but is capable of re-identification, as being within the scope of the law.[20]

In British Columbia, however, recent amendments to the *Freedom of Information and Protection of Privacy Act* indicate a willingness for legislation that gives business flexibility and a greater competitive edge.[21] Federally, on the other hand, it appears there may be some willingness to follow the GDPR's lead. The federal government had proposed to introduce a prohibition against re-identifying data in the *Consumer Privacy Protection Act* ("*CPPA*"), but was not clear whether de-identified data would be subject to the *CPPA*.[22] Due to the calling of the September 2021 election, the *CPPA* was not passed into law. As the federal government has not yet reintroduced similar legislation following the election, we cannot say with certainty at this time whether there will again be a prohibition against re-identifying data, but the OPC has suggested that pseudonymous data could fall within the current provisions of *PIPEDA*.[23]

Many companies are attempting to mitigate this risk by using, selling, or otherwise sharing only a small subset of data, arguing that by providing incomplete data sets, those seeking to re-identify an individual related to such data set cannot be sure the right person was identified.[24] However, these risks can arise even where the data set is largely incomplete.[25] Thus, companies who collect and use anonymized data should consider the means by which they are anonymizing their data to reduce the risk of re-identification and, in turn, potential liability for its collection, use, and disclosure.

The legislation and requirements around the protection of personal information and the techniques available to anonymize such personal information are constantly evolving. As a result, it is difficult for businesses to currently know for certain whether a particular approach will be acceptable going forward. Moving forward, it is important that businesses carefully analyze each opportunity or suggested approach in light of the current requirements and with a full review and assessment of the potential ways in which any such anonymized or aggregated data may be re-identified to ensure that it has taken all reasonable steps to remain in compliance with all privacy requirements.

If you have any questions or concerns regarding your business' use of anonymized and/or aggregated data, we recommend reaching out to our Privacy and Data Protection team.

A CAUTIONARY NOTE

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.

[***Robert C. Piasentin*** *delivers practical legal advice that drives the success of his clients' leadership, governance and strategic negotiation initiatives. He has contributed to the growth of a wide range of businesses in Canada, the United States and England. His strong commercial practice encompasses technology outsourcing transactions, software development and licensing solutions, strategic IP and technology commercialization arrangements, and privacy and cybersecurity issues.*

Kristen Shaw *recently graduated from the Peter A. Allard School of Law (Allard) at the University of British Columbia. While at Allard, she was a member of the BC Law Schools Moot Team, participated in the Corporate Counsel Externship through a placement with Equinox Gold Corp, and worked as a research assistant to Professor Alexandra Flynn.*]

---

1 Charlotte A. Tschider, "Regulating the Internet of Things: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age" (2018) 96:1 Denv U Law Rev 87 at 104, 107.

2 *Personal Information Protection Act*, S.B.C. 2003, c. 63 [PIPA], ss. 6-9.

3 *Personal Information Protection Act*, S.B.C. 2003, c. 63 [PIPA], s. 1. Ministry of Citizens' Services, "Guide to the *Personal Information Protection Act*", online: https://www2.gov.bc.ca/assets/gov/business/business-management/protecting-personal-information/pipa-guide.pdf.

4 *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, s. 2(1).

5 Gilad Rosner, "De-Identification as Public Policy" (2020) 3:3 Journal of Data Protection & Privacy 1 at 3-4.

[6] Charlotte A. Tschider, "Regulating the Internet of Things: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age" (2018) 96:1 Denv U Law Rev 87 at 105.

[7] The optimal state between anonymization and open use is often referred to as the "Goldilocks principle"; see Gilad Rosner, "De-Identification as Public Policy" (2020) 3:3 Journal of Data Protection & Privacy 1 at 7.

[8] Charlotte A. Tschider, "Regulating the Internet of Things: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age" (2018) 96:1 Denv U Law Rev 87 at 107.

[9] Scott R. Peppet, "Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security, and Consent" (2014) 93 Texas Law Rev 85 at 93-94.

[10] Scott R. Peppet, "Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security, and Consent" (2014) 93 Texas Law Rev 85 at 93-94.

[11] Scott R. Peppet, "Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security, and Consent" (2014) 93 Texas Law Rev 85 at 121-122.

[12] Charlotte A. Tschider, "Regulating the Internet of Things: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age" (2018) 96:1 Denv U Law Rev 87 at 96.

[13] Scott R. Peppet, "Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security, and Consent" (2014) 93 Texas Law Rev 85 at 93.

[14] Scott R. Peppet, "Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security, and Consent" (2014) 93 Texas Law Rev 85 at 121.

[15] Scott R. Peppet, "Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security, and Consent" (2014) 93 Texas Law Rev 85 at 128-129.

[16] *Privacy review of the COVID Alert exposure notification application*, Office of the Privacy Commissioner of Canada, July 31, 2020.

[17] *R v. Spencer*, [2016] S.C.J. No. 43, [2016] 2 S.C.R. 204, 2016 SCC 43.

[18] Scott R. Peppet, "Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security, and Consent" (2014) 93 Texas Law Rev 85 at 94.

[19] Luc Rocher, Julien M. Hundrickx & Yves-Alexandre de Montjoye, "Estimating the success of re-identification in incomplete data sets using generative models" (2019) 10 *Nature Communications* 3069; see also Arvind Narayanan & Vitaly Shmatikov, "Robust De-anonymization of Large Sparse Datasets" (2008), IEEE Symposium on Security and Privacy, pp 111-125 and Arvind Narayanan & Vitaly Shmatikov, "Robust De-anonymization of Large Sparse Datasets: a Decade Later" (2019) unpublished research paper, online: https://www.cs.princeton.edu/~arvindn/publications/de-anonymization-retrospective.pdf.

[20] See *General Data Protection Regulation* (EU), 2016/679, recital 75; Data Protection Working Party, "Opinion 05/2014 on Anonymisation Techniques" (2014), Technical Report, Article 29, online: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf#page=3 at 10.

[21] Bill 22, *Freedom of Information and Protection of Privacy Amendment Act, 2021*, 2nd Sess, 42nd Parl, British Columbia, 2021 (first reading) [Bill 22].

[22] See Bill C-11, *An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts*, 2nd Sess, 43rd Parl, Canada, 2020 (first reading) s. 75.

[23] *A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act*, Policy and Research Group of the Office of the Privacy Commissioner of Canada, May 2016.

[24] See Gregory J. Matthews & Ofer Harel, "Data confidentiality: a review of methods for statistical disclosure limitation and methods for assessing privacy" (2011) 5 Stat Surv 1-29 (2011); Daniel Barth-Jones, "The 're-identification' of Governor William Weld's medical information: a critical re-examination of health data identification risks and privacy protections, then and now" (2012), online: *SSRN Electronic Journal*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2076397.

[25] Luc Rocher, Julien M. Hundrickx & Yves-Alexandre de Montjoye, "Estimating the success of re-identification in incomplete data sets using generative models" (2019) 10 *Nature Communications* 3069 at 2.