Special Committee to Review the
Personal Information Protection Act

MODERNIZING BRITISH COLUMBIA'S PRIVATE SECTOR PRIVACY LAW

December 2021

LEGISLATIVE ASSEMBLY
of BRITISH COLUMBIA

Report
Second Session, 42nd Parliament

LEGISLATIVE ASSEMBLY
of BRITISH COLUMBIA

December 6, 2021

To the Honourable
Legislative Assembly of the
Province of British Columbia

Honourable Members:

I have the honour to present herewith the Report of the Special Committee to Review the Personal Information Protection Act.

Respectfully submitted on behalf of the Committee,

Mable Elmore, MLA
Chair

CONTENTS

COMPOSITION OF THE COMMITTEE

Members

First and Second Sessions, 42nd Parliament

Mable Elmore, MLA, Chair
Vancouver-Kensington

Dan Ashton, MLA, Deputy Chair
Penticton

Garry Begg, MLA
Surrey-Guildford

Kelly Greene, MLA
Richmond-Steveston
(from March 1, 2021)

Adam Olsen, MLA
Saanich North and the Islands

Rachna Singh, MLA
Surrey-Green Timbers
(to March 1, 2021)

Andrew Wilkinson, Q.C.
Vancouver-Quilchena

Fifth Session, 41st Parliament

Rachna Singh, MLA, Chair
Surrey-Green Timbers

Dan Ashton, MLA, Deputy Chair
Penticton

Mable Elmore, MLA
Vancouver-Kensington

Adam Olsen, MLA
Saanich North and the Islands

Steve Thomson, MLA
Kelowna-Mission

Committee Staff

Susan Sourial, Clerk Assistant, Committees and Interparliamentary Relations

Lisa Hill, Committee Research Analyst

Jesse Gordon, Committee Researcher

Mary Newell, Administrative Coordinator

Stephanie Raymond and Mai Nguyen, Committees Assistants

TERMS OF REFERENCE

On April 13, 2021, the Legislative Assembly agreed that a Special Committee be appointed to review the *Personal Information Protection Act* (S.B.C. 2003, c. 63) pursuant to section 59 of that Act.

That the Special Committee shall have the powers of a Select Standing Committee and in addition be empowered to:

a. appoint of its number one or more subcommittees and to refer to such subcommittees any of the matters referred to the Special Committee and to delegate to the subcommittees all or any of its powers except the power to report directly to the House;

b. sit during a period in which the House is adjourned, during the recess after prorogation until the next following Session and during any sitting of the House;

c. conduct consultations by any means the Special Committee considers appropriate;

d. adjourn from place to place as may be convenient; and

e. retain personnel as required to assist the Special Committee.

That any information or evidence previously under consideration by the Special Committees appointed by order of the House on February 18, 2020 and December 9, 2020 be referred to the Special Committee.

That the Special Committee report to the House by December 8, 2021; and that during a period of adjournment, the Special Committee deposit its reports with the Clerk of the Legislative Assembly, and upon resumption of the sittings of the House, or in the next following Session, as the case may be, the Chair present all reports to the House.

EXECUTIVE SUMMARY

The *Personal Information Protection Act,* (S.B.C. 2003, c. 63) (PIPA) was adopted by the Legislative Assembly of British Columbia in 2003 and governs the collection, use and disclosure of personal information about individuals by private sector and non-profit organizations. The Act recognizes the right of individuals to control access to and the use of their personal information, as well as the need for organizations to collect and use personal information for legitimate and reasonable purposes. PIPA requires that a special committee of the Legislative Assembly conduct a review of the Act every six years. Previous statutory reviews took place in 2008-09 and 2014-15. PIPA has not been significantly amended since 2003.

The Special Committee to Review the Personal Information Protection Act was first appointed on February 18, 2020. The Committee launched a public consultation process but did not complete its work before the dissolution of the 41st Parliament. In the 42nd Parliament, the Committee was appointed on December 9, 2020 with a requirement to report to the Legislative Assembly on the results of its review by December 8, 2021. In the new Parliament, the Committee initiated a second public consultation process and held public hearings with government officials, the Information and Privacy Commissioner and stakeholders. Overall, the Committee heard 43 presentations and received 57 written submissions.

In reflecting on the input received, Committee Members established a set of guiding values focused on maintaining privacy as a right for all British Columbians; promoting consistency with provincial, federal and international legislation; ensuring adaptability with new technologies; and supporting British Columbia's innovators.

Committee Members highlighted the rapidly growing digital economy, the major changes to technology over the past 20 years, and the digital world that British Columbians live in today. While new technologies have transformed the economy and daily life, they also bring new risks and challenges for protecting privacy. The Committee concluded that PIPA must be modernized to safeguard rights for individuals and provide up-to-date provisions to ensure competitiveness for British Columbia's businesses.

The Committee's report makes 34 recommendations to modernize PIPA. Members stressed the importance of alignment and harmonization with the changing federal, provincial and international privacy landscape, including the European Union's *General Data Protection Regulation* (GDPR).

Members also focused on the critical importance of new provisions to deal with the rapidly changing digital economy and recommended changes to PIPA to reflect modern information processing practices and their impact on privacy.

The importance of meaningful consent was another area of priority with a particular focus on ensuring that individuals are aware how their personal information is being used. The Committee recommends new rules to ensure that individuals understand how organizations are collecting, using, and disclosing their personal information and that sensitive information, such as biometric data and information about children and youth, have explicit protections.

Members noted that British Columbia is the only jurisdiction in Canada whose privacy legislation does not require any mandatory notification in the event of a privacy breach. The Committee recommends that PIPA require organizations to promptly notify affected individuals and the Office of the Information and Privacy Commissioner of a significant privacy breach.

With respect to the right of individuals to access and control their information, Members recognized the importance of clarifying rules to ensure that British Columbians obtain access to their information in a timely and affordable way. The Committee recommends strengthened provisions regarding access requests, including fee schedules, timeframes, applicable information, enforcement, and consequences of failing to provide access to an individual's information, whether requested by an individual or a third-party organization on behalf of an individual. The Committee additionally recommends that individuals have

the right to obtain their own personal information from an organization in a structured, commonly used and machine-readable format at a cost no greater than the actual cost of fulfilling the access request; and a clarification of the legal obligations for third party data transfers.

With respect to employee personal information, the Committee recommends that the Act strengthen existing provisions and create a distinct section in the legislation related to employee privacy including: protections, including job protection, for employees who make a privacy-related complaint against their employer, as well as for any others who are witnesses; limits on, and notification of, the collection of employee data; and a requirement to post information regarding employee privacy rights and employer responsibilities in workplaces. Additionally, Members recommend that PIPA address the increased use of employee personal devices in the workplace, and the potential risks to the information of employers, employees, customers, and clients.

Committee Members agreed that it is more important than ever for health information to be properly safeguarded. The Committee recommends that new legislation be brought forward to govern the collection, use and disclosure of health information in the public and private sectors, ensure that PIPA and the *Freedom of Information and Protection of Privacy Act* (FIPPA) explicitly allow for the use of anonymized health data for public health and research purposes, and that PIPA and FIPPA be harmonized to facilitate sharing of personal information between government and healthcare practitioners in a manner that respects the privacy rights of clients and patients.

The Committee recognized the importance of effective oversight by the Information and Privacy Commissioner and recommends that PIPA ensure the Commissioner's ability to conduct audits to identify and investigate systemic issues, issue findings and orders, and ensure compliance with the Act. Committee Members also recommended that the Commissioner be provided with the power to levy administrative monetary penalties currently found under the Act against organizations found to be in violation of PIPA, proportional to the severity of the violation and that administrative monetary penalties be set at an amount that is a sufficient deterrent to contraventions of the Act.

THE WORK OF THE COMMITTEE

A Special Committee was first appointed to review the *Personal Information and Protection Act* (S.B.C. 2003, c. 63) on February 18, 2020. The Committee was unable to complete its work before the 41st Parliament was dissolved on September 21, 2020. Following the provincial general election in October 2020, and the start of the 42nd Parliament, the Legislative Assembly appointed a new Special Committee on December 9, 2020, and again on April 13, 2021, to complete the review of the Act. Pursuant to the motion adopted by the House, any information or evidence previously under consideration by the Special Committees appointed in February and December, stands referred to the current Special Committee which must submit a report, including any recommendations respecting the results of the review, to the Legislative Assembly by December 8, 2021.

Briefings

Committee Members received briefings from senior officials with the Ministry of Citizens' Services and the Office of the Information and Privacy Commissioner on the legislation and the wider privacy landscape on June 2, 2020, September 16, 2020, and February 23, 2021.

Kerry Pridmore, Assistant Deputy Minister and Chief Records Officer, Ministry of Citizens' Services, and Matt Reed, Executive Director of Privacy Compliance and Training, provided the Committee with a historical and cross-jurisdictional overview of privacy legislation and outlined the ten privacy principles underlying PIPA and noted their commonality across privacy legislation. The Executive Director also noted that the privacy landscape has shifted over the past decade, highlighting examples of new privacy legislation in California, Europe, and Canada which have been driven by many changes including rapidly evolving digital technologies; increased public scrutiny; and the increased severity and frequency of privacy breaches.

In response to input received during the Committee's 2020 public consultation regarding meaningful consent, modernization of PIPA, and the need to harmonize the Act with other jurisdictions, Ministry officials suggested there may be potential benefits to ensuring GDPR (*General Data Protection Regulation*) adequacy and regulatory consistency across Canada, including enhanced privacy rights and the need to support economic growth. They cautioned that it is beneficial to maintain PIPA's principle-based and technology neutral character. They encouraged reforms in relation to enforcement, including granting the Commissioner the power to initiate investigations without a complaint and make orders based on commissioner-initiated investigations. Committee Members also heard that PIPA could be amended to use gender neutral language to ensure that the Act is more inclusive.

Officials from the Ministry of Citizens' Services, and the OIPC provided a subsequent briefing related to Bill C-11, An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make related and consequential amendments to other Acts. Bill C-11 was drafted to align Canada's privacy legislation with the GDPR, and Ministry officials noted the importance of PIPA maintaining its "substantially similar" status when compared to federal privacy legislation. Organizations subject to a substantially similar provincial privacy law are generally exempt from the *Personal Information Protection and Electronic Documents Act* (S.C. 2000, c. 5) (PIPEDA) with respect to the collection, use or disclosure of personal information that occurs within their respective province. Ministry officials also suggested that the Committee consider the impacts that any recommendations may have on businesses and non-profits.

The Information and Privacy Commissioner for British Columbia, Michael McEvoy, joined by Deputy Commissioners, oline Twiss and Jeanette Van Den Bulk, also presented to the Committee. The Commissioner noted that since the legislation was first introduced 17 years ago, new technological developments, such as big data and artificial intelligence, have driven the need to update PIPA to continue to ensure robust privacy protection for British Columbians. The Commissioner also noted that demands for reform are driven both by improved European privacy standards, such as the GDPR, as well as a general heightened

public awareness of privacy threats and the need to protect personal information.

Though the OIPC has undertaken extensive outreach and education efforts and initiatives to inform businesses and individuals of their responsibilities under PIPA, the Commissioner believes that these efforts are not enough to properly protect British Columbians. The Commissioner warned that, while British Columbia's privacy legislation was seen as progressive when first introduced, PIPA is now lagging behind other jurisdictions. The Commissioner encouraged Members to consider recommending: the implementation of mandatory breach notification where there is a real risk of significant harm to an individual; alignment with provisions in PIPEDA and Alberta's PIPA; modernizing consent requirements to require clear and simple language; mandatory breach notification; and adequate enforcement provisions, such as administrative monetary penalties. The Commissioner urged the Committee to recognize that rapidly evolving digital technologies, business models and public attitudes towards privacy require a legislative response that is equal to the challenges faced.

In his presentation to the Committee on key provisions of Bill C-11, Commissioner McEvoy, noted that there were a number of provisions in Bill C-11 that were not fundamental to the substantially similar provisions that provinces are required to meet and should not be included in PIPA as they may not further the privacy rights of British Columbians. He highlighted 10 areas where PIPA should be reformed in line with Bill C-11, including: mandatory breach notification; third-party transfers; modernization of consent provisions; inclusion of a provision for the "right to be forgotten;" automated decision making; inclusion of a provision for the right to data portability; administrative monetary penalties; compliance agreements with organizations; improved cooperation with other data regulators; and enhanced oversight powers. He also highlighted the importance of Canada maintaining adequacy with the GDPR, describing the Regulation as "an absolute game-changer internationally," adding, "it dramatically raised privacy standards, and its reverberations have been felt well beyond Europe's borders." The Commissioner noted that as a trading jurisdiction, it is critical that British Columbia ensure that its personal information privacy laws are leading-edge and, to the greatest extent possible, harmonized with similar legislation nationally and internationally. Meeting GDPR standards will ensure that British Columbia is substantially similar to the federal legislation; he further told the Committee that there is no danger in the Committee making recommendations that push beyond the standards set in Ottawa.

Public Consultations

The Committee launched its initial public consultation during the 41st Parliament, on May 4, 2020, inviting British Columbians to provide their input by August 14, 2020; as part of their consultation, the Committee held three public hearings on June 9, 16 and 17, 2020. Following the provincial general election and the re-appointment of the Committee in the 42nd Parliament in December 2020, the Committee launched a second public consultation on May 18, 2021.

In light of the proposed federal legislative changes to the *Personal Information Protection and Electronic Documents Act* (PIPEDA) introduced in November 2020 in Bill C-11, An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make related and consequential amendments to other Acts, Committee Members requested that submissions focus on the provisions of Bill C-11 and the European Union's *General Data Protection Regulation* (GDPR) - which is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union - as well as on the input provided by the Information and Privacy Commissioner for British Columbia in his February 23, 2021 appearance before the Committee. The Committee held public hearings on June 22 and 23, and on July 6 and 7; the deadline for written submissions was July 30, 2021.

Over the course of its consultations, the Committee issued province-wide news releases announcing the launch of the consultations, placed advertisements in major provincial and community newspapers, and used social media and the Committee's website to promote the process. Overall, the Committee heard 43 presentations and received 57 written submissions. Lists of the individuals and organizations that made presentations and/or written submissions are available in Appendix A and Appendix B. The Committee wishes to thank all those who provided valuable input during the public consultations.

Meetings Schedule

Second Session, 42nd Parliament

April 16, 2021	Organization
June 22, 2021	Public Hearing (Virtual)
June 23, 2021	Public Hearing (Virtual)
July 6, 2021	Public Hearing (Virtual)
July 7, 2021	Public Hearing (Virtual)
October 1, 2021	Deliberations
October 4, 2021	Deliberations
October 12, 2021	Deliberations
October 14, 2021	Deliberations
October 19, 2021	Deliberations
October 21, 2021	Deliberations
October 28, 2021	Deliberations
November 2, 2021	Deliberations
November 16, 2021	Deliberations
November 18, 2021	Deliberations
November 23, 2021	Deliberations
November 26, 2021	Deliberations; Adoption of Report

First Session, 42nd Parliament

January 6, 2021	Organization
January 28, 2021	Organization
February 4, 2021	Organization
February 23, 2021	Briefings; Organization (Virtual)

Fifth Session, 41st Parliament

February 19, 2020	Organization
April 7, 2020	Organization
June 2, 2020	Briefings (Virtual)
June 9, 2020	Public Hearing (Virtual)
June 16, 2020	Public Hearing (Virtual)
June 17, 2020	Public Hearing (Virtual)
September 16, 2020	Briefings (Virtual)

THE STATUTORY FRAMEWORK

Section 59 of the *Personal Information Protection Act* (PIPA) requires a Special Committee to undertake a comprehensive review of the Act every six years. PIPA received Royal Assent in October 2003 and came into force on January 1, 2004. It requires private-sector organizations in British Columbia to protect and secure personal information that they have in their custody or under their control against unauthorized use or disclosure, and grants individuals the right to access their own personal information and to request corrections if they think their information is incorrect or incomplete. The Act was amended in 2004, 2006 and 2007. A minor "housekeeping" amendment was made in 2016.

British Columbia, Alberta and Quebec all have private sector privacy laws that have been deemed substantially similar to the *Personal Information and Protection of Electronic Documents Act* (PIPEDA), the federal privacy legislation which applies to federal works, undertakings, or businesses, and to interprovincial or international transfers of personal information. PIPEDA also applies to provinces that do not have their own privacy legislation.

Related Legislation

The *E-Health (Personal Health Information Access and Protection of Privacy) Act* (S.B.C. 2008, c. 38) came into force on May 29, 2008. The purpose of the Act is to provide legislative authority and a privacy framework to protect personal health information contained in designated health information banks (HIBs) of the Ministry of Health or health authorities.

Statutory Reviews

Since 2004, there have been two statutory reviews of PIPA undertaken by special committees of the Legislative Assembly, the first in 2007-2008 and the second in 2014-2015.

2007-2008 Statutory Review

The 2007-2008 review concluded that the Act was generally working as intended. The Committee's report made 31 recommendations to: enhance accountability for cross-border data flows; require mandatory notification of privacy breaches; prohibit the use of "blanket" consent forms by provincially regulated financial institutions; increase oversight, particularly in relation to the dispute resolution process for privacy complaints; and provide the Commissioner with the authority to discontinue a complaint or request for review if they believe the complaint or request is without merit or where there is not sufficient evidence to proceed.

2014-2015 Statutory Review

Similar to the initial review of the Act, the Committee's report concluded that PIPA was effectively serving the privacy interests of British Columbians. The Committee made 15 recommendations to: enhance accountability, improve protections for the collection, use and disclosure of information; respond to certain court decisions; improve breach notification requirements and provisions for disclosure without consent; clarify an organization's responsibility for personal information after transmittal and access rights; and improve the oversight authority of the Information and Privacy Commissioner. The Committee also recommended that the provincial government publicly respond to the Committee's recommendations and provide an implementation plan in a timely manner.

GUIDING VALUES FOR THE COMMITTEE

As the Committee undertook its deliberations on the input received during its public consultations and briefings, Committee Members agreed to a set of guiding values, including a rights-based approach to information privacy, to frame their deliberations and the development of their recommendations.

Purpose of the Act

British Columbians have the right to privacy and protection of their personal information which may only be infringed by consent or operation of law. The *Personal Information Protection Act*'s (PIPA) stated purpose (Part 1, Section 2) is to govern the collection, use and disclosure of personal information by non-governmental organizations in a manner that recognizes both the right of individuals to protect their personal information and the need for organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

Committee Guiding Values

1. **Privacy is a Right:** supports a rights-based approach to privacy and the protection of personal information for British Columbians.
2. **Accessible and Clear:** written in plain language and understandable for individuals, companies and organizations.
3. **Transparent:** privacy policies and practices, as well as privacy officer contact information should be easily accessible and understandable; processes for accessing, changing or removing someone's personal information or making a privacy complaint should be easy to do.
4. **Modern and Consistent:** reflective of the current digital landscape and consistent with provincial, federal and international legislation and good practices.
5. **Harmonized and Interoperable:** privacy requirements should be harmonized and interoperable with other provinces across Canada and internationally.
6. **Proportional and Fair:** requirements and penalties should be proportional, fair and reflective of the size of the organization and balance the need for effective regulation with the need for manageable and workable obligations for small organizations and companies.
7. **Flexible and Technologically Neutral:** principles-based and technologically neutral to apply widely and be adaptable to new technologies.
8. **Supportive of BC's Innovators:** support innovation in British Columbia's digital economy while recognizing the right of individuals to protect their personal information.

Principles of Privacy Protection

Developed by the Canadian Standards Association (CSA), the 10 Principles of Privacy Protection are also known as the Model Code for the Protection of Personal Information and were recognized as a national standard in 1996. In 2000, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) incorporated and gave the force of law to the CSA's principles. The principles outline the rights and obligations of individuals regarding the access and use of their personal information and of the private organizations that collect, use, store and disclose that information. The principles contain common features found in most privacy legislation around the world, including in the European Union's GDPR: the GDPR's "Principles of Privacy Protection" mirror the CSA's principles.

The principles were incorporated into PIPA at its inception to inform the way private organizations collect, secure, use and disclose personal information. The Office of the Information and Privacy Commissioner (OIPC) refers to the principles in their guidance document entitled *Developing a Privacy Policy Under PIPA* which outlines organizational obligations for handling personal information. Additionally, the provincial government encourages organizations to become familiar with the principles in order to develop, implement and maintain an appropriate privacy program.

10 PRINCIPLES OF PRIVACY PROTECTION	GDPR PRINCIPLES OF PRIVACY PROTECTION
1. Accountability	1. Lawfulness, fairness and transparency
2. Identifying purpose	2. Purpose limitation
3. Consent	3. Data minimization
4. Limiting collection	4. Accuracy
5. Limiting use, disclosure and retention	5. Storage limitation
6. Accuracy	6. Integrity and confidentiality (security)
7. Safeguards	7. Accountability
8. Openness	
9. Individual access	
10. Challenging compliance	

Modernization of the Act

PIPA needs to reflect the current privacy landscape and ensure that the personal information of British Columbians is protected by robust privacy legislation. While the purpose of PIPA to protect privacy and individual liberties is important, the Committee recognized that personal privacy is a much broader concept than confidentiality which involves protecting personal information and also limiting when and how it is collected and used. Modern day privacy legislation needs to reconcile the fundamental and sometimes competing values of protection of privacy and the free flow of information to provide needed services to British Columbians and support businesses, including the transborder data flows that contribute to socioeconomic development.

During the review process, it became clear to Committee Members that the Act requires substantial amendments to situate it as an effective piece of legislation in the current privacy landscape. The Committee also acknowledged the importance of aligning PIPA with privacy legislation in other jurisdictions and recognized that the GDPR is the current internationally recognized "gold standard" for privacy legislation. As such, the Committee was of the view that PIPA needs to be modernized to embrace the concepts that form the basis of the GDPR, as well as harmonize with other provincial and federal privacy legislation. In the interest of highlighting the overall purpose of PIPA and to raise awareness among British Columbians, the Committee recommends that the 10 Principles of Privacy Protection be highlighted and made more visible within the Act.

The Committee also expects that government will engage with Indigenous stakeholders regarding any amendments to the Act as per the *Declaration on the Rights of Indigenous Peoples Act*, (S.B.C. 2019, c. 44) which was adopted by British Columbia in November 2019.

THE PRIVACY LANDSCAPE

In 1999, the Legislative Assembly of British Columbia appointed the Special Committee on Information Privacy in the Private Sector to examine, inquire into and make recommendations with respect to the protection of personal information in private sector transactions, and the impact of electronic documents on privacy and freedom of information for British Columbians. The Committee cited innovations in information and surveillance technologies such as smart cards, keystroke monitoring, biometric identification systems, and health information systems to demonstrate the need for British Columbia to have its own standalone private sector privacy legislation. The recommendations made by the Committee led to the introduction of the *Personal Information Protection Act*. The world has changed substantially since the Committee's report was adopted: social media was largely limited to chatrooms and blogs; the biometric identification systems noted by the Committee have become integrated into technologies on a scale that was at the time unimaginable; cellphones were mostly used to make and receive calls and texts; and the "internet of things" was not yet conceptualized.

New innovations and digital technologies, such as the proliferation of social media, the pervasive integration of mobile devices into day-to-day activities, advancements in biometrics and in Artificial Intelligence (AI), have embodied a social, economic, and technological shift not seen since the industrial revolution. In many ways, these technologies have made the lives of British Columbians easier, such as how automated decision making (ADS) systems are used to expedite the process of applying for loans, jobs, or insurance. However, the algorithms that drive ADS systems can be programmed with subconscious biases, which can result in individuals being automatically denied access to products or services as a result of their race, sexual orientation, religion, or gender.

In the last 20 years, data has become central to almost everything we do as a society and this increased importance is reflected in its value as a commodity to be collected, shared and sold. With this recognition comes a host of other issues including bad actors and criminals who flagrantly violate an individual's privacy for profit, fail to provide adequate safeguards, or attempt to exploit systems to access our personal data.

At the center of these issues is the collection, use and disclosure of personal information. In response, jurisdictions around the world have modernized their privacy legislation to both protect their citizens from the increasingly apparent threats to their privacy, and to support the need for businesses to safely innovate in their sectors. The European Union's GDPR provides some of the most stringent privacy provisions internationally. At its heart, the GDPR recognizes that individuals, rather than organizations, own their information and should exert control over it. The GDPR gave regulators improved mechanisms of enforcement, and informed other countries that they could not access the data of EU subjects unless they also had adequate privacy laws that reflected GDPR's core principles. Soon after the introduction of the GDPR, jurisdictions such as Australia, Brazil, Japan, and the United Kingdom all enacted, reviewed or revamped their privacy legislation in response. In the United States, Illinois and California have also introduced new legislation to help better protect the privacy of their citizens.

Canada has also begun engaging in the process of updating its privacy legislation. In 2020, the federal government introduced Bill C-11 which proposed some provisions around modernizing consent requirements; regulating automated decision-making systems; and strengthened financial penalties for violations, though the bill was not adopted before Parliament was prorogued for a federal election. In the fall of 2021, Québec adopted *An Act to modernize legislative provisions as regards the protection of personal information*, which was designed to align with the GDPR. The Act introduced the most stringent privacy laws in Canada, including stronger fines; mandatory breach notification; mandatory privacy impact assessments; new consent requirements; a privacy by design requirement; a right to data portability; and new rules about anonymization of personal information. In addition, Ontario recently undertook a public consultation on privacy legislation and released their *White Paper on Modernizing Privacy in Ontario*. The paper included proposed provisions to strengthen privacy rights for

Ontarians such as more safeguards for artificial intelligence (AI) technologies; dedicated protections for children; updated consent rules to reflect the modern data economy; the promotion of responsible innovation and correcting the systemic imbalances between individuals and the organizations that collect and use their data.

British Columbia has a strong and innovative tech sector, which contributed $18.3 billion to its GDP from 2018 to 2019. Failing to address the changing privacy landscape will leave this sector at a disadvantage on the global stage and British Columbia will be unable to attract new innovative companies. Failing to update our privacy laws also leaves British Columbians susceptible to serious privacy threats. The Committee's review of PIPA and its resulting recommendations provide a unique opportunity to shape PIPA into a modern, flexible, clear, fair, and harmonized "made in British Columbia" legislation that protects the privacy rights of its citizens and supports innovation in British Columbia.

ALIGNMENT AND HARMONIZATION WITH OTHER PRIVACY LEGISLATION

The European Union's GDPR was brought into force in 2018 and includes various provisions for the protection of personal data of EU citizens and also addresses the transfer of personal data outside the EU. The Regulation also enhances an individual's control and rights over their personal data and simplifies the regulatory environment for international organizations.

On November 17, 2020 the federal government introduced Bill C-11, which proposed many substantial changes to PIPEDA to bring Canada further into alignment with the GDPR while focusing on strengthening privacy protection for consumers and providing a set of rules to ensure fair competition in the online marketplace. Committee Members sought input on Bill C-11 during the Committee's 2021 public consultation process in the interest of aligning PIPA with this proposed federal legislation to ensure that British Columbia retained its "deemed substantially similar" status.

General Data Protection Regulation (GDPR)

Daniel Therrien, Privacy Commissioner of Canada stated that "while Canada used to be a leader in privacy protection, and unfortunately, the world is now passing us by. Many jurisdictions worldwide have taken steps to enhance their privacy laws to better protect their citizens. The GDPR is the most notable example of legislative modernization in recent years that has raised the 'privacy bar' worldwide." The GDPR outlines 99 articles and 173 recitals detailing the legal obligations of organizations when they process the information of European citizens. The articles outline the legal requirements of organizations, and the recitals provide additional information and context to support the articles. Commissioner Therrien went on to say that Canada, at both the provincial and federal levels, should take meaningful action to enhance its privacy laws and regain its reputation as a global privacy leader to not only enhance protection of individuals' rights and promote trust in commercial activities, but to also help promote inter-operability between jurisdictions, providing predictability and potential cost savings to Canadian businesses. In his presentation to the Committee, Commissioner Therrien encouraged Committee Members to look at the GDPR as a source of inspiration while amending PIPA to suit the privacy protection needs of British Columbians.

The Retail Council of Canada noted that it is absolutely critical to maintain adequacy with the GDPR and proposed that any future amendments to the legislative framework take this into account. The Canadian Council of Innovators also suggested that the Committee make recommendations to align PIPA with the GDPR in terms of personal privacy and data protection. The BC Freedom of Information and Privacy Association noted that Canada's adequacy status with the GDPR must be confirmed by May 2022 and that provincial sub-jurisdictions are subject to adequacy scrutiny. The economic impacts of a non-adequacy assessment could have significant implications for British Columbia, including on economic development and innovation.

In his presentation to the Committee, Dr. Colin Bennett indicated that Bill C-11 would likely not meet GDPR adequacy requirements. He suggested that the Committee reform PIPA to meet GDPR adequacy, noting that if PIPA broadly meets GDPR standards, then it will likely meet adequacy requirements of any new federal legislation.

Bill C-11, An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make related and consequential amendments to other Acts

In his February 2021 submission entitled *PIPA Reform and Proposed CCPA Provisions* as well as in his presentation to the Committee on February 23, 2021, the Information and Privacy Commissioner for British Columbia, Michael McEvoy, outlined 10 aspects of Bill C-11 that align with his previous suggestions for PIPA reform as outlined on pages 8-9 of this report. Representatives from the Ministry of Citizens' Services provided a briefing to the Committee on February 23, 2021 during which they provided a presentation on Bill C-11 and the

GDPR, including the most notable provisions of both statutes and the impacts on and obligations of organizations. Regarding implications for British Columbia, Ministry officials stressed the importance of alignment between provincial and federal privacy legislation, particularly in terms of how this might affect the viability of provincial organizations and businesses.

In his presentation to the Committee, Privacy Commissioner Therrien noted that Bill C-11 would represent a step back for privacy protection as, while the bill sought to address most of the privacy issues relevant in a modern digital economy, it did so in ways that were frequently misaligned and less protective than the laws of other jurisdictions. Commissioner Therrien provided the Committee with a number of proposed amendments to Bill C-11 as part of his submission and urged Committee Members to look at the GDPR for potential amendments to PIPA. Commissioner Therrien also proposed that the Committee consider a human-rights based approach to data protection and indicated that this would widen the lens for how we understand, interpret and apply those provisions that are designed to protect individuals from exploitation and abuse in a data-driven society. In agreement, the BC Freedom of Information and Privacy Association advocated for the Committee to recognize privacy as a fundamental human right and adopt a human rights-based approach within PIPA, noting that Canada is a signatory of the *Universal Declaration on Human Rights* and Article 17 of the *International Covenant on Civil and Political Rights*, and both of these declarations recognize privacy as a human right.

In her presentation to the Committee, Dr. Teresa Scassa noted that both the GDPR and Bill C-11 are stimuli for reforming British Columbia's PIPA. She suggested that the various limitations of Bill C-11 may be because of the constitutional constraints placed on the federal government, and that as a province British Columbia will be able to push beyond the federal bill. She added that personal data is no longer the by-product of the relationship between a business and a customer, but rather is now a commodity in its own right: personal data is mined, processed, analyzed, shared, sold, and exploited in a myriad of new ways. Dr. Scassa proposed the Committee help British Columbia set its own course and look beyond Bill C-11 to ensure the best privacy protection possible for British Columbians.

Harmonization with Federal and Provincial Legislation

The Canadian Marketing Association stated that "PIPA has many strengths that have stood the test of time. It is built on solid principles that provide flexibility for specific applications, and its framework is understandable and achievable for non-specialists." They also noted that many features of PIPA provide materially better privacy outcomes for individuals than newer and more prescriptive laws in other jurisdictions. Jade Buchanan, a lawyer and certified information privacy professional, indicated that the complex network of distinct jurisdictions for privacy legislation means that businesses have a difficult time knowing their privacy obligations across Canada. It also means that business practices that are legal in other provinces could be a violation under British Columbia's PIPA.

A number of organizations highlighted the need to harmonize protocols for mandatory breach reporting, including the Canadian Civil Liberties Association, the Canadian Bankers Association, and the BC Government Employee and Service Union. Specifically, these organizations advocated for making changes to ensure that compliance is an easier process for organizations already familiar with Alberta's PIPA and PIPEDA. Jade Buchanan suggested that provincial and federal Privacy Commissioners should collaborate to explore the benefits of implementing a unified mandatory breach notification process across all Canadian jurisdictions.

In their presentation to the Committee, the Canadian Life and Health Insurance Association noted that many British Columbia companies do business across Canada and that having separate and potentially incompatible legislation could potentially hinder their ability to expand to other provinces. As businesses begin to bounce back from the economic hardships created by the COVID-19 pandemic and direct their efforts towards economic recovery, it is essential that there is regulatory coordination across all jurisdictions so as not to impose an additional burden on businesses. In his presentation to the Committee, the Information and Privacy Commissioner stated that the timeframe for amendments to the federal legislation remains unclear.

Freedom of Information and Protection of Privacy Act (FIPPA) and PIPA

The BC Civil Liberties Association and the BC Freedom of Information and Privacy Association indicated that there is a perceived legislative gap between the *Freedom of Information and Protection of Privacy Act* (R.S.B.C. 1996, c. 165) (FIPPA) and PIPA in instances where public sector organizations outsource work to private sector organizations. They further noted that private sector organizations can share information or collect information with public sector organizations in ways that would not be legal under FIPPA, and these private sector organizations are not subject to FOI requests in the same way as public sector organizations. The British Columbia Teachers' Federation suggested that PIPA and FIPPA should be harmonized to facilitate bargaining relationships between public sector employers and unions. Similarly, the British Columbia Dental Association indicated that the harmonization of PIPA and FIPPA would facilitate the flow of information between government ministries and dental offices. This alignment would help to ensure that the dental services provided are in alignment with a ministry client's coverage limits, helping to limit out-of-pocket expenses incurred by patients.

Committee Discussion

Committee Members were particularly interested in the European Union's GDPR, noting that many have described the GDPR as a leading example of modern privacy and personal data protection legislation. They considered how provisions withing the GDPR might apply to a "made in BC" approach to modernizing PIPA and noted that British Columbia should focus on prioritizing interoperability with the GDPR. The Committee highlighted the importance of ensuring that PIPA meets the GDPR's adequacy requirements, not only in terms of taking a leadership role, but also to ensure that British Columbia's economy and business sector can remain competitive, and that British Columbia is seen as an attractive location for technology companies to locate.

Committee Members also stressed the importance of PIPA continuing to meet the "substantially similar" requirements of any federal privacy legislation. The Committee also wanted to ensure that PIPA harmonizes with similar privacy legislation in other provinces to make it easier for companies that operate across Canada to comply with inter-provincial privacy requirements and encourage the growth of British Columbia business across the country.

RECOMMENDATIONS

The Special Committee recommends to the Legislative Assembly that the provincial government:

1. Ensure that PIPA meets GDPR and anticipated federal adequacy requirements.
2. Update PIPA with a focus on prioritizing interoperability with other provincial and international legislation, including the GDPR.

NEW AND EMERGING TECHNOLOGIES

In the last decade, there have been considerable changes and innovations related to technology that have significant socio-economic and privacy impacts. Stakeholders identified a range of issues related to the privacy impacts including data de-identification, automated decision-making systems, biometrics, and the impact that these aspects may have on economic development. PIPA does not include provisions to address any of these aspects specifically; however, the legislation has thus far been able to provide adequate protection due to its technology neutral language. Federally, some of these issues have been addressed in PIPEDA, such as defining biometric information as sensitive information and Bill C-11 included provisions for automated decision-making systems, and de-identification of personal information. The GDPR has articles dedicated to automated decision-making systems, recitals related to the handling of pseudonymized and anonymized data, and defined biometric information as sensitive information, requiring more stringent protections and consent.

De-Identified Information or Anonymization

PIPA currently has no provisions to explicitly differentiate de-identified information from other types of information. However, the legislation was designed to be principles based and technology neutral, relying on a reasonableness standard rather than prescriptive rules. De-identified information is sometimes referred to as "anonymized" and is the process by which data is stripped of its identifying characteristics, which could include an individual's name, age, location, or gender, among other identifiers. Once the identifying information has been removed, PIPA allows for the data to be reused for various purposes. PIPEDA has already recognized that "de-identified data" should be considered "personal information" if there is a "serious possibility" that the data could be re-identified.

The BC Civil Liberties Association indicated that although de-identification of personal information is promoted as an effective means of protecting privacy, the increasing amount of information collected from individuals and the growing sophistication in data collection, data linking, data analytics and artificial intelligence, increase the risks of re-identification of an individual's personal information. The BC Freedom of Information and Privacy Association (FIPA) added that very little information that is classified as de-identified is actually de-identified, noting that there are numerous examples of data being "anonymized" only to be re-identified later. In their joint submission, FIPA and the BC Civil Liberties Association (BCCLA) suggested that that de-identified data be included within the scope of PIPA and should be treated on a contextual basis, based on a variety of factors such as: the nature of the data; the intended purposes for its use; the availability of other linkable data; the likely incentives to re-identify the data; the costs and level of expertise required to re-identify data; and the potential harm to individuals should an individual be re-identified.

Conversely, the BC Tech Association suggested that de-identified information should continue to be excluded from the definition of personal information under PIPA, and instead, regulations could be adopted that would prohibit re-identifying information to provide continued support for tech innovation and relief for consent-fatigued individuals. Trans Union of Canada, Inc. also noted that privacy laws should only extend to personal information but expressed an openness for the development of a policy framework to promote de-identification for industry innovation and to be able to leverage data for socially and economically beneficial purposes while ensuring an appropriate level of privacy protection for individuals.

Tech Nation indicated that the GDPR includes descriptions for both pseudonymization and anonymization and noted that pseudonymization is the processing of personal data in such a way that the data can no longer be attributed to a specific individual without the use of additional information. Unlike anonymization, pseudonymization techniques do not exempt data controllers from the GDPR; however, it does help with data protection obligations, including data minimization and storage limitation, and processing for research purposes for which appropriate safeguards are required.

The Canadian Bar Association noted in their submission that Bill C-11 defined "de-identify" as "to modify personal information – or create information from personal information – by using technical processes to ensure that the information does not identify an individual or could not be used in reasonably foreseeable circumstances, alone or in combination with other information, to identify an individual." The Canadian Marketing Association (CMA) indicated that de-identification and pseudonymization of personal information are longstanding techniques that are commonly used by organizations and are hallmarks of protecting individual privacy. The CMA further noted that Bill C-11's definition of 'de-identify' was so broad that it appeared to place restrictions on any data that was ever derived from personal information, a concern shared by the Insurance Bureau of Canada. The Canadian Bankers Association expressed concern that Bill C-11's broad prohibition on re-identifying information could halt the practice of using pseudonymization to safeguard personal information.

The Canadian Civil Liberties Association noted that Bill C-11 did not succeed in making it clear that de-identified data was within the scope of Bill C-11, nor did it clearly outline the limits on its appropriate use. ISACA suggested that pseudonymization of data should be a mandatory practice to better protect personal information.

Automated Decision-Making Systems

Artificial Intelligence (AI) is a catch-all term that encompasses automated decision-making systems (ADS), algorithmic sorting, and machine learning. All of these processes relate to a computer algorithm receiving or collecting information, processing and sorting the information, and then using that information to perform a function. In 2021, the Centre for Digital Rights indicated that AI has enabled major leaps forward in innovation; however, these technologies can pose serious risks to the privacy of British Columbians. The Canadian Civil Liberties Association (CCLA) noted that ADS is not a neutral process, and it often has inherent biases that can negatively impact the individuals about whom the decision was made. The BC Freedom of Information and Privacy Association agreed, noting that individuals may be unaware when ADS was involved in making decisions that have an impact on them or have no concept of the factors considered by ADS to arrive at decisions. Indeed, these algorithms are sometimes referred to as a 'black box' because even their creators often do not know how the decisions were reached. ADS can also be used to influence and target individuals' behaviour without their knowledge through advertising. The CCLA noted that everyone should have the ability to opt out of ADS if they wish. Commissioner McEvoy told the Committee that these technologies are evolving at a rate that poses challenges for appropriate regulation; and British Columbia needs to make sure that PIPA properly contemplates the increasing use of AI and ADS.

The Insurance Bureau of Canada agreed that ADS may pose some risks to the privacy of individuals; however, these risks could be mitigated through regulations, rather than allowing individuals to opt out of ADS. There are also benefits of ADS for the average consumer, including a reduction in the hours needed to process insurance claims, finding the best protection plan for individuals, and reducing the overall cost of insurance. The Canadian Wireless Telecommunications Association noted that the potential harms of ADS are already addressed under other regulatory frameworks such as competition, consumer protection and human rights legislation. Trans Union of Canada, Inc. proposed a more meaningful policy review of ADS focused on what information should be used to enable individuals to be made aware of how decisions are made about them, including what specific information is considered.

Elizabeth Denham, UK Information Commissioner and former Information and Privacy Commissioner for British Columbia, pointed out that the GDPR enables individuals to object to the automated processing of their personal data. Former Information and Privacy Commissioner for British Columbia, David Loukidelis, submitted that Québec's *Act to modernize legislative provisions respecting the protection of personal information* requires organizations to be transparent about ADS, but noted that the Act does not require organizations to consider an individual's input or provide other protections against ADS. He indicated that the potential of automated systems is clear, but more effective limits, such as those in the GDPR, are necessary to achieve a better balance between individual rights, and business and other socially beneficial interests. He also suggested that the provincial government create an expert working group to "assess current trends in artificial intelligence and, following meaningful public consultations, make recommendations for an artificial intelligence regulatory framework in British Columbia."

Provisions in Bill C-11 would have addressed ADS by requiring organizations to provide a general account of their use of automated decision-making systems to make predictions, recommendations or decisions about an individual that could

have significant impacts on them. However, Commissioner McEvoy expressed some concerns, arguing that Bill C-11 did not go far enough in regulating this kind of activity while also noting that the GDPR approach goes too far. The CCLA agreed that Bill C-11 did not go far enough, noting that the bill included openness provisions that required organizations to make a general account of the organization's use of any ADS that could have significant impacts on individuals, and also included access provisions which entitled an individual to an explanation of how their personal information was used to make a decision. However, it failed to provide any recourse should individuals wish to contest the use of their information for this purpose.

The Canadian Life and Health Insurance Association stated that Bill C-11 would have adequately protected individuals, based on the obligation to provide a general account of ADS and the right to obtain further details through an access request. The Canadian Marketing Association and the Canadian Bankers Association noted that transparency requirements are helpful but warned that restrictions on the use of ADS will put British Columbia organizations at a competitive disadvantage.

Economic Development and Innovation

Dr. Colin Bennett noted that the global privacy landscape has changed substantially since 2004 when PIPA came into force; since then, personal information has become one of the most valuable resources. He suggested that strong privacy laws can support a robust modern economy and indicated that PIPA has become outdated, which has the potential to leave British Columbia at a significant disadvantage from a global economic perspective. Canada's Digital Technology Supercluster noted that the Organization for Economic Co-operation and Development scores Canada as 12th out of 16 nations for innovation. They suggested that British Columbia engage in a comprehensive, holistic review of PIPA to better prepare its digital economy for the future and ensure that any new or updated legislation is dynamic and responsive. Although they believe that international standards will significantly dictate the substance of a new privacy law, Canada must seek opportunities to set itself apart as an attractive place to innovate. Commissioner McEvoy noted that British Columbia is being left behind as provincial, federal and international legislators modernize their privacy laws to respond to the shift to digital economies, and to also meet the challenges posed by technologies such as artificial intelligence, data analytics, facial recognition, and social media. He also told the Committee that updated privacy legislation could have considerable economic benefits for British Columbia, particularly in light of British Columbia's technology sector, which generates billions of dollars annually.

In his submission to the Committee, Greg D'Avignon of the Business Council of British Columbia noted that during the COVID-19 pandemic, e-commerce sales in Canada nearly doubled, with a majority of Canadians who made e-commerce transactions indicating they intend to continue to make online purchases once the crisis has passed. He noted that this is a complex and nuanced legal and policy area, in which most consumers care about privacy, but are happy to share extensive personal information to gain access to digital services and goods. This is often referred to as a 'privacy paradox.' The BC Tech Association emphasized the essential role that privacy legislation plays in protecting the rights and privacy of citizens; however, there is also the possibility that stringent privacy regulation can stifle innovation, which highlights the importance of striking the right balance between protection of privacy and the need for businesses to collect, use and disclose information, while also recognizing that any changes to privacy laws can have lasting consequences for businesses. The Canadian Vehicle Manufacturers' Association echoed this and suggested that certain sectors, such as automotive manufacturing, are already regulated by government at a federal level, and also by numerous private sector working groups that safeguard the privacy of consumers. They noted that industry needs a clear and consistent privacy landscape to support innovation and drive investment, and that additional regulations on certain sectors could be detrimental.

The BC Tech Association highlighted that when the GDPR was implemented, its stringent rules made it difficult for many smaller businesses to compete with the larger, more established technology firms. They noted that many new technologies, and novel uses for existing technologies, have emerged in the last 15 years that may not have been possible if innovators were stifled by stringent regulations. Trans Union of Canada also indicated that privacy frameworks require clear principles which must be nimble and aligned with major trading partners, technologically neutral, and should embrace common sense rules that apply to the collection, use, disclosure, retention and security of personal information. Jade Buchanan proposed that before any new regulations come into effect, there be a sufficient transition period to provide organizations time to update or review their practices and policies.

Biometrics

The Canadian Civil Liberties Association noted that the private sector is increasingly engaged in expanding the collection of biometric data, from facial recognition to fingerprints. Often data collection is facilitated by confusing privacy policies, or ones that may allow over-collection of information beyond reasonable or intended purposes. According to the CCLA, this highlights a regulatory gap and lack of power for the Commissioner. Other jurisdictions are stricter; for example, Illinois legislation requires explicit written consent for the collection of biometric data, or even a total prohibition on the collection of biometric data, such as facial recognition in public places. In their submission, Ian Linkletter noted that increasingly this type of information is used in educational institutions. Another individual noted that, unlike other types of information, once facial and other biometric data is compromised, it is irreversible; one cannot change this information the way one could change a password.

Committee Discussion

While discussing the issue of de-identification, Members recognized the benefits of this process for the purposes of research and innovation and noted the important scientific innovations that can be achieved with access to these types of datasets. However, the Committee also expressed concerns about the potential risks involved and agreed that such provisions need to be clearly legislated to ensure adequate safeguards are in place. Members noted the input they received suggested that Bill C-11 did not provide clear enough definitions on this topic and agreed that more precision was needed in any definitions adopted in British Columbia's PIPA. Any definitions related to de-identification should be technology neutral and avoid prescribing specific measures or processes.

The Members appreciated the clarity provided by the GDPR's description of pseudonymization, which is "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person." If the information cannot reasonably be attributed to an identifiable person, it is anonymous and not within the scope of the legislation. Members noted that the GDPR provides an explanation of what is "reasonably" in Recital 26 which is "to ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments." The Committee agreed that both definitions are forward looking and technology neutral. Members also agreed that pseudonymized information should be included within the scope of PIPA. As anonymization is a difficult standard to achieve and technological processes are constantly evolving, Members felt a prohibition on re-identifying information without authorization would help ensure the safety of anonymized and pseudonymized information.

Members noted that AI is prevalent in our everyday lives and it includes things like internet browser search functions, software in a smart toothbrush, technology in self-driving cars, and the programming logic content streaming services use to suggest movies based on user preferences. The Committee wanted to encourage organizations to continue to innovate with new technologies and was cognizant that limitations on automated processing may result in increased costs for routine goods and services which will likely be passed on to consumers. As such, Members noted that any legislative changes attempting to regulate these systems need to be carefully considered.

Conversely, the Committee expressed concerns about ADS, noting the serious potential negative implications of the use of these algorithms and indicated that individuals should be made aware that an automated system may be making decisions about them. Members were particularly concerned about the risk of latent bias in these algorithms and noted that these systems cannot be expected to perform the same tasks as human beings. They indicated that an awareness of this risk was demonstrated by legislation to regulate ADS in other jurisdictions, noting that the GDPR requires notification of automated processing, including profiling, and an option to object to the processing upon request. The GDPR also includes certain exemptions to this requirement.

Recognizing that any regulation in this area could have far reaching economic and social consequences and noting the complexity of the potential benefits and drawbacks of AI and ADS, the Committee recommended that this is an important issue that should be addressed. Reflective of the advice received from the former Information and Privacy Commissioner for British Columbia, the Committee would like to see further studies undertaken, including a public consultation, to inform any proposed amendments to the Act.

The Committee also discussed the importance of up-to-date privacy legislation, in-step with other jurisdictions, recognizing that PIPA is in need of updates, without which British Columbia would be at a significant economic disadvantage. Members agreed that the business community needs stability and consistency to continue developing innovative technologies and products.

Committee Members expressed concerns about the sensitivity of biometric information, noting that once this type of information is compromised there is no way to secure it again. The Committee indicated that this makes biometric data unique among types of personal information, and special considerations must be provided for its collection, use, and disclosure; additionally, individuals need to be aware of what organizations are doing with their biometric data and have control over how it is used.

RECOMMENDATIONS

The Special Committee recommends to the Legislative Assembly that the provincial government:

3. Ensure that PIPA include definitions of pseudonymized information as personal information, and anonymized information as outside the scope of PIPA, similar to definitions in the GDPR.
4. Ensure PIPA prohibits the re-identification of pseudonymized or anonymized information by any person, organization, or contractor other than the originally authorized person, organization, or contractor.
5. Ensure that PIPA requires an organization to notify an individual that automated processes were used to make a significant decision about them and includes provisions to allow an individual to request human intervention in the decision-making process.
6. Require organizations to reaffirm the consent of individuals to collect, use, disclose, or process biometric data with reasonable frequency.
7. Explicitly require an organization to delete biometric information within a reasonable timeframe upon the request of an individual.

The Special Committee recommends to the Legislative Assembly that the Office of the Information and Privacy Commissioner:

8. Undertake a public consultation to study the long-term socioeconomic impacts of artificial intelligence, including automated decision making and automated profiling, and provide the Ministry of Citizens' Services with any recommendations for proposed amendments to the Act.

MEANINGFUL CONSENT

Meaningful consent is foundational to how individuals exert control over their own personal information. However, privacy legislation differs on what types of data collection require consent, and what type of consent is required. PIPA currently permits organizations to obtain consent in one of three ways: express or explicit consent - in which consent is provided verbally or in writing; deemed consent - in which consent can be reasonably assumed and the purposes are obvious; and consent by not declining. Section 12 of PIPA also outlines several exemptions to consent.

The GDPR provides various exemptions for consent and mandates that all data collection needs to be guided by a principle of "privacy by design" to demonstrate that privacy protection was a primary consideration. The GDPR also outlines a special category of information called sensitive personal information, which requires explicit consent from individuals.

Commissioner McEvoy suggested that PIPA's definitions of consent were largely drafted for bilateral agreements, in which an individual provides their information to a single organization for a specific purpose; however, this definition may no longer be sufficient to address current complex data ecosystems. Many organizations, such as the Canadian Civil Liberties Association (CCLA), BC Tech Association, BC Civil Liberties Association (BCCLA), and the BC Freedom of Information and Privacy Association (FIPA), suggested that in the past decade, PIPA has become inadequate to address the challenge of increasing privacy threats in British Columbia. Commissioner McEvoy noted that as information technology has evolved, many digital services have become integral to modern life. Dr. Theresa Scassa noted that organizations are frequently relying on complicated privacy policies that at times may obscure the scope and purposes of collection. Dr. Andrew Clement agreed, adding that the collection of information is increasingly monetized. The amount of freely available information has led LandlordBC to submit that it is not reasonable or realistic to restrict a landlord's ability to search for publicly available information about potential tenants on the internet.

The BCCLA and BC FIPA reported that 67 percent of Canadians feel little to no control over how their personal information is used by companies, as was demonstrated by one individual who was frustrated to learn that their car's service record was uploaded to a central system without their knowledge. One student expressed concern about increasing, and seemingly compulsory, integration of digital technologies into the daily school activities of students. Another individual noted that proctoring software has seen increased use throughout the COVID-19 pandemic. Students are often not provided an alternative means to take that test and cannot meaningfully consent to the system's sometimes invasive facial recognition software. The Centre for Digital Rights noted that political parties also collect and use significant amounts of personal information in their political outreach, and that this has become more common with the proliferation of big data technology.

The BC NDP pointed out that political parties are unique because they do not fit into either the private or public sector. In British Columbia, political parties are covered under PIPA; however federally, no such provisions exist. FIPA suggested that political outreach should continue to be regulated under PIPA and they support the OIPC's recommendations outlined in its investigative report entitled *Full Disclosure: Political parties, campaign data, and voter consent,* which included recommendations to address limitations on the collection of voter information; transparency about voter profiling; limits on the collection of publicly available information; and stronger information security practices. In their submission, the BC Green Party stated that it does not think that exemptions to consent are necessary for political parties.

In 2018, the OIPC introduced guidelines regarding meaningful consent, stipulating that meaningful consent means that an individual is provided the essential elements of: what information will be collected; what will be done with it; and how the collection is reasonable. The information must be accessible and easily understood, and there needs to be a clear option to accept or reject the collection of data. FIPA and the

BCCLA suggested that the concept of "meaningful consent" needs to be codified in PIPA. The Insurance Bureau of Canada opposed the idea and the Canadian Marketing Association raised concerns that meaningful consent may cause "consent fatigue," a term used to describe individuals being overwhelmed by the amount of information provided in consent agreements, resulting in them not reading the policy.

The BC Tech Association indicated that the GDPR outlines six conditions in which an organization can process (rather than collect, use or disclose) information: performance of a contract; compliance with a legal obligation; vital interest of the data subject; public interest; legitimate interest; and with consent. However, Dr. Bennett submitted that the GDPR also implemented a privacy by design requirement which imposes an obligation on the data controllers to implement appropriate technical and organizational measures so that privacy preserving measures, such as data minimization or pseudonymization is built into the plan for data collection, use, and disclosure prior to implementation.

In Bill C-11, the federal government wanted to achieve a balance between business interests and privacy by adopting several new exceptions to consent. Commissioner Therrien noted that while some of these exceptions are reasonable, others are ill-defined. Commissioner McEvoy agreed, noting that consent exemptions in Bill C-11 were not a good model for British Columbia. Dr. Andrew Clement noted that the current model for consent in Canada is not working and expressed concerns that Bill C-11 would not adequately weigh the importance of privacy and that the draft legislation has removed the reasonableness standard for implied consent.

The Canadian Wireless Telecommunications Association stated that the exemptions are too rigid and prescriptive, while the BC Tech Association expressed concerns about the impact of changing consent requirements for small businesses and technology firms. Jade Buchanan suggested that if the rules around consent in PIPA are changed, organizations should be allowed to grandfather in consent already obtained. The Chartered Professionals in Human Resources BC stated that the current language of the Act works well.

Committee Discussion

Members expressed concerns about overly complex consent agreements, and echoed stakeholder concerns about individuals who may experience "consent fatigue." The Committee recognized that there is a strong need to protect the privacy of British Columbians through appropriate consent provisions; however, each new requirement has the potential to be onerous on small businesses and non-profits during an already challenging time. In addition, Members felt that the current system of consent is not effective as current privacy policies can be overly complex and opaque, leaving British Columbians at a disadvantage. The Committee recognized that it is important to ensure that individuals are fully aware of what personal information is collected, how it is collected, and what will be done with it.

Members noted that the GDPR includes numerous exemptions to consent, and that these exemptions are grounded in a privacy by design requirement. They also noted that the six exemptions to consent outlined in the GDPR are clear, accessible, and fair compared to the situationally specific exemptions currently outlined in PIPA. The Committee expressed support for the idea of a privacy by design requirement but were concerned that this would be too burdensome for small and mid-sized businesses and non-governmental organizations. Members thought that a guidance document issued by the OIPC explaining the importance and benefits of privacy by design might be helpful for organizations.

Members discussed the importance of special protections for sensitive categories of information, including information relating to children and youth, biometrics, political views, religion, sexual orientation, and medical information, noting that such provisions were included in the GDPR, and as such, they would like to see PIPA updated to require explicit consent and data handling practices for sensitive data. The Committee expressed concerns about the damage that social media can do, and has done, to young people, specifically in relation to negatively influencing and manipulating teenagers.

RECOMMENDATIONS

The Special Committee recommends to the Legislative Assembly that the provincial government:

9. Update the requirements of explicit consent to include meaningful consent provisions.

10. Align the exemptions to consent in PIPA with those of the GDPR.

11. Define new sensitive categories of information in PIPA which would require explicit consent from individuals and specific data handling practices to include: biometric data, political views, religion, sexual orientation, medical information, and information related to children and youth.

The Special Committee recommends to the Legislative Assembly that the Office of the Information and Privacy Commissioner:

12. Develop guidance information explaining the importance and benefits of the principles of "privacy by design."

MANDATORY BREACH NOTIFICATION

PIPA currently does not require an organization to notify individuals following a data breach of their information; however, some organizations may choose to do this as a best practice. In comparison, the GDPR requires data controllers to report serious data breaches to "a proper supervisory authority" within 72 hours. Québec's *An Act to modernize legislative provisions respecting the protection of personal information* requires mandatory breach notification "as soon as feasible."

In 2020 Commissioner McEvoy noted that there was a dramatic increase in the number and magnitude of privacy breaches in the private sector in Canada, noting that the federal Privacy Commissioner estimated that 28 million Canadians were affected by a privacy breach in 2018, which represents approximately 70 percent of the population. Commissioner McEvoy indicated that PIPA should be amended to require mandatory breach notification where there is a real risk of significant harm to an individual. He noted that with the enactment of Québec's new privacy law, *An Act to modernize legislative provisions as regards the protection of personal information*, British Columbia is the only province whose private sector privacy legislation does not require mandatory notification once an individual's personal information has been breached. The Commissioner added that this should be supported by the ability to levy administrative monetary penalties, as simply "naming and shaming" organizations will not result in sufficient compliance.

The Privacy Commissioner of Canada, Daniel Therrien, noted in his June 2021 presentation to the Committee that mandatory breach notification ensures individuals are able to take steps to protect themselves if their personal information may have been compromised. Commissioner Therrien suggested that PIPA be amended to require organizations to report a breach without unreasonable delay - ideally, within seven days after they become aware of the incident. Commissioner Therrien told Committee Members that an effective regulator must be properly equipped with meaningful powers that lead to quick and effective remedies and that there needs to be real consequences for organizations and businesses that break the law and incentives to comply, noting that Bill C-11 included a provision for the Commissioner to issue orders to organizations in relation to privacy violations and recommend administrative penalties up to three percent of global turnover or $10 million, for a limited list of key infractions. Bill C-11 also included a provision for the creation of an administrative tribunal empowered to implement administrative monetary penalties.

A number of individuals and organizations, including the Office of the Information and Privacy Commissioner of Alberta, suggested that any amendments with respect to mandatory breach notification and reporting should use "real risk of significant harm" (RROSH) as the threshold for reporting a privacy breach to avoid "breach fatigue" among the public. "Breach fatigue" occurs when individuals receive frequent breach notifications which can foster complacency and lessen the impact of these notifications over time. Implementing a threshold would also ensure that the most serious breaches are reported immediately to the Commissioner, including: identity theft; financial loss; humiliation; damage to reputation or relationships; loss of employment, business or professional opportunities; negative effects on a credit record; damage to or loss of property; and the risk of bodily harm. A number of other stakeholders echoed the concerns regarding breach fatigue, as well as a potential increase in the number of breach notifications that the OIPC would have to deal with. Canada's Digital Technology Supercluster expressed concerns about overburdening the OIPC with numerous reports of minor privacy breaches, but they want to ensure that the privacy of British Columbians is protected. The Canadian Bar Association, BC Branch, wanted to ensure that any amendment to PIPA regarding mandatory breach reporting has a single threshold for reporting to the OIPC and to affected individuals and suggested the Committee consider whether noncompliance with mandatory reporting obligations should result in meaningful financial consequences to organizations.

Although Ontario does not currently have privacy legislation that is substantially similar to the *Personal Information Protection and Electronic Documents Act* (PIPEDA), the Information and Privacy Commissioner of Ontario noted that their *Personal*

Health Information Protection Act includes mandatory breach reporting and administrative monetary penalties. While the requirement to notify individuals of a data breach has been in place since 2004, the Act was further amended in 2017 to include a threshold for the Ontario Commissioner to be notified. Depending on the scope and implications of a particular breach, it should be noted that not every privacy breach that requires an individual to be notified requires the Commissioner to also be notified. After the 2017 amendment came into force, the number of privacy breaches reported to the Commissioner increased significantly. In addition, health data custodians in Ontario are required to produce annual reports on privacy breaches, which must include privacy breaches that did not meet the threshold to report to the Commissioner, such as instances of misdirected faxes or unauthorized access by medical professionals.

Committee Discussion

The Committee noted that British Columbia is currently the only province in Canada whose private sector privacy legislation does not require any mandatory notification in the event of a privacy breach. Expressing concerns about the increasing severity and frequency of privacy breaches, Committee Members want to ensure that British Columbians are not only made aware of a privacy breach in a prompt and timely manner, but that they are also able to take appropriate actions, such as updating their security measures, as soon as possible to minimize the implications and potential damages arising from the breach. Considerations of proportionality and reasonableness were important considerations for the Committee, including the severity of the breach and whether "breach fatigue" might affect individuals.

Committee Members considered the provisions in the GDPR which require data controllers to report serious data breaches to a proper supervisory authority within 72 hours unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. Committee Members discussed the importance of consistency regarding mandatory breach notifications in the interest of harmonizing PIPA with other jurisdictions and increasing awareness of the risk of privacy breaches among British Columbians.

Committee Members also discussed the current methods by which an individual might receive a breach notification and were concerned that individuals might not receive an urgent notification if it is only delivered via a single method of communication, such as an email that may end up in an individual's junk mail folder. In the interest of improved communications, the Committee wanted to see the Act amended to allow for various direct methods of breach notification, including email, text, phone call or regular mail, in particular for notification of serious privacy breaches where individuals need to be informed that their personal information is at risk.

RECOMMENDATIONS

The Special Committee recommends to the Legislative Assembly that the provincial government:

13. Include provisions in PIPA similar to those in other jurisdictions to require organizations to promptly notify the OIPC and affected individuals of a privacy breach, with consideration for proportionality regarding the severity of the breach.

14. Ensure that PIPA allows for various direct methods of communication to notify affected individuals of a breach, including email, text, phone call or regular mail.

DISCLOSURE OF PERSONAL INFORMATION

PIPA currently does not include provisions related to data portability, or data protection impact assessments; however, it does require the deletion of information once the purposes for which it was collected have passed and stipulates that individuals must receive a copy of their information upon request.

The GDPR includes several provisions to enhance the control individuals have over their own personal information. For example, Article 15 provides an individual the right to access their information; Article 20 provides an individual the right to receive their information in a portable manner; Article 17 provides individuals the right to have their information deleted; and Article 35 requires organizations to undertake a data protection impact assessment. The GDPR also includes rules and provisions for transferring information to third parties.

Bill C-11 did not require privacy impact assessments; however, it did propose a right to disposal, and a limited right to data portability which required that an organization "disclose the personal information that it has collected from the individual to an organization designated by the individual, if both organizations are subject to a data mobility framework provided under the regulations."

Access Requests and Fees

Section 23 of PIPA provides that, upon request, an individual must receive access to their personal information under the control of the organization and several stakeholders spoke of the difficulty of gaining that access. The Donald R. McLeod Law Corp. indicated that many organizations delay access, create barriers, or charge significant processing fees to individuals attempting to legally access their records. These barriers can limit those who do not have the time or knowledge of the Act from enacting their rights.

Conversely, some organizations noted the difficulty of processing access requests. The Insurance Bureau of Canada indicated that PIPA currently permits organizations to charge only a minimum fee for processing access requests, which has sometimes meant that organizations are charging less than the resources required to fulfill the access request. The Canadian Life and Health Insurance Association expressed frustration over the abundance of 'frivolous claims,' which they described as individuals using access rights under PIPA to avoid having to pay the normal processing fees for access to personal information requests.

Section 23 of PIPA allows organizations to refuse to disclose information related to access requests for several reasons, including if the disclosure could harm a commercial organization's competitive advantage. In both 2020 and 2021, the BC NDP noted that some candidates are submitting access requests to opposing political parties to probe for any personal information that may have been collected as part of routine campaign activities. The BC NDP noted that Section 23 (3)(b) allows an organization to refuse to disclose information that would reveal confidential commercial information that would harm the competitive position of the organization. They noted that the Commissioner determined that this provision does not apply to political parties because their activities are not "commercial." However, the BC NDP stated that elections are highly competitive environments, and though their activities may not be commercial, responding to access requests by political opponents can harm their competitive position. The BC NDP proposed that Section 23(3)(b) be amended by removing the word "commercial"; they further proposed that the Act "treat candidates as organizations, rather than individuals, for the purpose of access to information requests related to their candidacy."

Currently, there is no provision under Section 23(3) of PIPA that permits an organization to withhold information for the purposes of litigation privilege. The Insurance Bureau of Canada raised concerns that individuals may be making requests for access and correction of their personal information for the purpose of frustrating an insurance claim. The BC Teachers Federation expressed similar concerns regarding union business.

Other organizations also highlighted issues with the misuse of access requests. The BC Society of Transition Houses noted that they help women, children and youth experiencing domestic and sexual violence, stalking, trafficking and harassment by providing individuals with safety and employment planning, in-person and online services, and referral supports. They also provide psychoeducational counselling programs for children between the ages of three and 18 and their non-offending caregivers. As part of this work, they collect sensitive information about these individuals and their family situations, including personal information about the offending caregiver, which can be subject to access requests by family members during family court processes and criminal proceedings. Increasingly, transition houses have undertaken considerable expense to litigate against these access requests, which are generally dismissed by the courts.

The Health Science Association of British Columbia highlighted that Section 23(4)(c) of PIPA requires an organization to redact, or refuse to disclose, information if its disclosure would reveal personal information about another individual; should an individual request access to their own information, and their file includes information about another individual, the organization must redact it, regardless of the circumstance. In contrast, FIPPA requires that a public body refuse to disclose personal information if the disclosure would be an "unreasonable invasion" of a third-party's personal privacy. The Health Science Association of BC indicated that a similar provision in PIPA would be helpful.

Data Portability

Data portability is an individual's right to request their information from an organization in a transportable and easily-readable format. This provides an individual more choice in determining which organizations best serve their needs and demonstrates that data is owned by the individual, not the organization.

Currently there are no requirements related to data portability in PIPA; however, it is included in the GDPR and was proposed in Bill C-11. The GDPR's data portability right includes the right to port data "in a structured, commonly used and machine-readable format." Bill C-11 differentiated personal information from proprietary information; the latter was not portable. Dr. Theresa Scassa noted that constitutional restraints may have limited the scope of data portability in Bill C-11, rather than the broad, open-ended portability seen in the GDPR.

The Canadian Wireless Telecommunications Association noted that Bill C-11 would have required both organizations involved in the transfer to be subject to a data portability framework and noted that the inability to easily transfer personal information to an alternate service would have presented a barrier to switching service providers. Dr. Andrew Clement stated that ideally, portability would allow for interoperability between service providers and added that by defining data portability as a data subject's right, and by not imposing the stringent conditions that Bill C-11 would have imposed, the GDPR does a much better job of attempting to enable portability. Rogers Communications stated that such provisions do not belong in privacy legislation and the Retail Council of Canada suggested that data portability should be limited to personal information created by individuals such as emails, photos, or posts, and does not extend to all types of data held by organizations.

Dr. Mike Figurski, an expert in health data stewardship, submitted that a major problem some physicians face is the portability of digitized patient records, noting that many data storage venders only provide unsearchable file formats, such as PDF, making it difficult to exchange information. The Insurance Bureau of Canada noted that data portability provides some unique challenges, such as a heightened risk of third parties of dubious intent accessing data on behalf of an individual. They further suggested exploring an industry specific consultation process to examine the best way for each industry to adapt to data portability. The Canadian Marketing Association suggested that if stipulations regarding data portability were added to PIPA, an organization should not be required to delete the data immediately after transferring the information to the individual.

Data Storage and Destruction

PIPA requires organizations to maintain personal information records for at least one year after they have used that information and that the information must be destroyed afterwards. Landlord BC expressed concerns that, due to the volume of information that they collect on prospective tenants, the one-year retention period is too long, and they want to see the time shortened for rental applications. The International Secure Information Governance and Management Association (I-SIGMA) identified the lack of safeguards organizations use in the destruction of personal information and noted that a major source of privacy

breaches is due to negligence in the destruction process. In addition, the current wording of Section 35(2) of PIPA may lead some individuals to incorrectly believe that once a name of an individual is removed from a document, the document may be disposed of, when in fact additional steps may be required to ensure that the remaining information cannot be re-identified, even if the document no longer contains an individual's name.

The Right to be Forgotten

Once publications are posted online and indexed in a search engine, they are easily accessible and difficult to remove. To address this, some jurisdictions have enacted a "right to be forgotten" provision in their privacy legislation which allows individuals, in certain circumstances, to remove information that is damaging or inaccurate from the internet. The GDPR's Article 17 provides for the right to erasure and provides individuals the right to request the deletion of any information related to them, including publicly accessible information, if certain conditions are met, as well as information that is held by organizations.

The Canadian Marketing Association noted that PIPA requires organizations to destroy personal information or render it unidentifiable as soon as the purposes for which it was collected have passed. The Canadian Bankers Association noted that PIPA contains protections against using outdated and inaccurate information, while the BC Teachers Federation expressed concerns that a right to be forgotten stipulation could be detrimental for litigation purposes and could negatively impact labour disputes. Additionally, the Global Automakers of Canada noted that the federal *Motor Vehicle Safety Act* and the *Canadian Environmental Protection Act* may require manufacturers to keep records despite a destruction request. Both MediaSmarts and the Canadian Bar Association supported the prospect of a public consultation on the implementation of the right to be forgotten in British Columbia.

Some organizations told the Committee how helpful such a provision would be to them, including the Mortgage Brokers Institute/Canadian Mortgage Brokers Association which noted that careers can be ruined by online registries of brokers who have been publicly disciplined. The Insurance Bureau of Canada were in favour of individuals having control over their own information but added that there needs to be exemptions such as the detection of fraud, or for internal modeling purposes.

Privacy Impact Assessments

The BCCLA, the Freedom of Information and Privacy Association (FIPA), and Dr. Colin Bennett suggested that privacy impact assessments (PIAs) should be mandatory for all organizations who collect, use, or disclose an individual's personal information. PIAs are reports that organizations submit to regulators which outline all of the possible privacy risks a proposed change may pose. The frequency, content, and reporting requirement of PIAs should be defined by regulations and the OIPC could provide PIA templates for organizations to provide guidance on what is expected (similar to PIAs under FIPPA). The BCCLA and FIPA acknowledged that PIAs can be expensive for small businesses but emphasized the benefits of a robust privacy management program which can be more cost effective, both reputationally and financially, than dealing with a breach. To balance costs, the content and frequency of a PIA can vary depending on the sensitivity and volume of personal information. Requiring mandatory PIAs will provide more transparency for corporations, bring PIPA more in line with other jurisdictions, and also serve an important role of providing an early warning system to regulators of possible privacy risks so they may advise on mitigation strategies. The Canadian Marketing Association noted that privacy policy requirements should not be too prescriptive, such as requiring organizations to include specific and standardized information or language in their privacy notices, as such privacy policies do not result in better consumer understanding.

Fraud

Pacific Blue Cross has found that while investigating claims of fraud, some healthcare providers obstruct or delay investigations by stating that they cannot provide treatment records to verify their billed services unless Pacific Blue Cross obtains additional express consent from their patients. Pacific Blue Cross is also aware of cases in which patients declined to provide additional consent because they were colluding with the providers in submitting improper claims. The Insurance Bureau of Canada noted a potential contradiction in PIPA as it does not explicitly allow for the collection, use, or disclosure of information without consent for the purposes of managing an insurance claim; however, there are other sections which explicitly state that collection without consent is acceptable for the purposes of an investigation. The Insurance Bureau of Canada, the Canadian Life and Health Insurance Association, and Pacific Blue Cross put forward various ideas about how best

to amend Section 18 of PIPA to address the issue of detecting fraud.

The former Information and Privacy Commissioner for British Columbia, David Loukidelis, outlined that Sections 12(1)(c), 15(1)(c), and 18(1)(c) of PIPA stipulate that an organization can collect, use, and disclose personal information without consent if it is reasonable to expect that the consent of the individual would compromise the availability or accuracy of the personal information or compromise an investigation or proceeding, and the use is reasonable for purposes related to an investigation or a proceeding. He noted that PIPA outlines several exemptions to consent, which acknowledge the balance between protecting individual privacy and an organization's need for personal information. Several safeguards exist within the Act to ensure that personal information collected, used, or disclosed during the course of an investigation or proceeding is reasonable. First, the definition of "Investigation" in Section 1 of the Act stipulates that an organization can only collect, use or disclose information related to an investigation where it is reasonable to believe that certain kinds of wrongdoing have occurred. Second, PIPA only allows organizations to collect, use, or disclose information if a reasonable person would consider it appropriate in the circumstances. Third, any personal information collected, used, or disclosed by an organization during the course of an investigation must be reasonable for the investigation or proceeding. He outlined that these three safeguards ensure that an investigation is only conducted for reasonable purposes, and any information collected during the course of the investigation is reasonable. He added that requiring organizations to also determine if the consent of an individual would compromise the availability or accuracy of the personal information is an undue burden on organizations. He suggested that PIPA should be amended to permit organizations to collect, use, and disclose personal information where it is reasonable for the purposes of an investigation.

Third-Party Data Processing

Many organizations rely on contractors to perform various business functions that involve the personal information of customers or clients, including payroll processing or providing cloud-based services. Under Canadian privacy laws, the accountable organization is responsible for ensuring that personal information under its control is subject to appropriate safeguards. In the context of data processing by a service provider, it is the accountable organization that either identifies the safeguards that a service provider must meet or determines that the service provider's security standards meet the accountable organization's requirements. Unlike legislation in other jurisdictions, PIPA currently does not expressly hold businesses responsible for how their contractors protect personal information. The Canadian Life and Health Insurance Association suggested Section 34 of PIPA already requires an organization to safeguard the information under their control, thereby providing sufficient protection. The Canadian Marketing Association proposed that, given the commonality and frequency of data flows, government should preserve the current model, which does not require additional consent for third-party transfers, and provides adequate privacy protection. Trans Union of Canada Inc. agreed, and noted that such data transfers should be facilitated, rather than hindered, by privacy legislation.

The Canadian Marketing Association raised questions about the obligations of third-party service providers. In their 2019 report, *Joint investigation of AggregateIQ Data Services Ltd.*, the OIPC and Office of the Privacy Commissioner of Canada found that AggregateIQ was negligent because they failed to verify the consent of individuals whose information they were handling on behalf of their client. This decision by the Commissioners diverges from the common assumption that British Columbia companies are subject to the laws of their client's jurisdictions rather than the laws of British Columbia. This decision creates an obligation for British Columbia companies who process data to be in alignment with PIPA, even outside the province. The Ministry of Citizens' Services warned that such an obligation may create significant barriers for businesses to compete on a global scale.

The Centre for Digital Rights noted that PIPA's lack of cross-border data rules represents a significant gap in the legislation. Dr. Andrew Clement told the committee that PIPA is outdated in its understanding of data handling and unable to support current data supply chains. This is in part because the Act takes too narrow a view of both the range of roles that organizations play within the data ecosystem and the widely varied data processes they engage in. Dr. Clement stated that the GDPR does a much better job of reflecting current realities and holding all the actors in data supply chains accountable, including definitions of data controller and data processor roles.

Bill C-11 included provisions to improve transparency for third-party data processing, but Dr. Clement noted that it failed to solve the problem of opaque transfers, as it only included the

term "service provider," rather than "data controller or data processor," which did not reflect modern data practices. The bill would also have required an organization to disclose whether they carried out any international or interprovincial transfer or disclosures that may have had reasonably foreseeable privacy implications. TECHNATION noted that Bill C-11 would have imposed a standard for security on service providers that is overly burdensome.

Committee Discussion

During their discussion, Committee Members agreed that the current provisions in PIPA related to the detection of fraud are too limiting and noted that this may be an issue for many organizations. The Committee stressed the importance of balancing the detection of fraud with the privacy of individuals, and that any expanded powers to investigate fraud need to recognize this. The Members noted that the concerns raised by former Information and Privacy Commissioner David Loukidelis related to fraud investigations could have wider implications on areas such as access to information requests, data retention, and data destruction, and wanted to ensure that nothing in the Act would hinder a criminal or fraud investigation.

While the Committee understands the concerns raised by stakeholders regarding the issue of vexatious access requests, Members noted that the principle of access to information is important to British Columbians and agreed that individuals should be provided with their information at a reasonable cost and within a practical timeframe. Of particular concern to the Committee was the number of access requests to organizations that help persons fleeing domestic violence, such as women's shelters. Members noted that other jurisdictions include clear exemptions to access requests for records related to areas such as: child abuse data; regulatory functions relating to legal services, health services, and children's services; crime and taxation; and confidential references. These individuals are in extremely vulnerable positions and PIPA should have additional protections related to accessing confidential records of this nature. Citing similar provisions in other jurisdictions, the Committee agreed that individuals should be able to request their information from an organization for a reasonable fee. Members further agreed that the Act should continue to maintain certain exemptions to access requests, such as information related to proprietary information, and information related to criminal or fraud investigations.

One of PIPA's strengths has been its neutrality towards technology, thus making the legislation adaptable to change, in particular in relation to the definition of methods of data destruction. However, the Committee agreed that PIPA should continue to require organizations to destroy information as soon as the purpose for which it was originally collected has ended, or by the time the organization is no longer required by law to maintain their records. The Committee noted that because of some of the legal obligations related to records retention as provided in the *Limitation Act* (S.B.C. 2012, c. 13) information can be retained for significant lengths of time. In addition, Members indicated that PIPA should be updated to outline baseline requirements for destruction, and that individuals should know how their information will be safeguarded and how it will be destroyed.

The right to be forgotten as outlined in the GDPR covers both online posts, as well as the information that a company holds about individuals. Regarding the deletion of online public information, the Committee expressed concerns that the right to be forgotten could be widely abused by individuals trying to delete records of past crimes. However, regarding the application of the 'right to be forgotten' to children and youth, the Committee noted that the mistakes of youth are far more public now than in previous decades and suggested there should be a mechanism for removal of information, photos, or videos that were posted to social media with or without consent. This concern was especially pronounced for sexually explicit images and videos posted without consent, an issue that can affect people of all ages. The Committee also noted that other jurisdictions have adopted right to be forgotten provisions in their privacy legislation, and a more fulsome investigation of the topic is required.

It is critical to keep large organizations accountable for their data privacy practices without overburdening small and medium-sized businesses or non-governmental organizations. The GDPR requires organizations to conduct a data protection impact assessment prior to processing information with a high degree of risk; this sets a good example for corporate transparency and demonstrates that an organization has a privacy plan in place to protect sensitive information. Members agreed that such an approach balances protecting highly sensitive information while ensuring that organizations are not overburdened. Committee Members noted that a template could be provided by the OIPC to ease the process of creating a privacy impact assessments (PIAs).

Members reflected on the input received related to third-party data transfers noting that PIPA needs to align with other jurisdictions and explicitly outline the responsibilities of organizations when transferring data to the data controller. The data controller is responsible for personal information they collect from individuals and it is up to organizations to determine how to best safeguard this information.

Members discussed the issue of whether the sale of personal information to third parties should be reflected in an individual's file when they request access to it. The Committee took note of the increased monitoring of social media profiles by organizations for data brokering and marketing purposes, recognizing that this is a widespread societal problem. The posts and tweets of individuals can be monitored, collected, and analyzed and the surveillance of social media to collect this information is indicative of a lack of control that individuals have over their information. The Members felt that both the federal and provincial privacy commissioners should provide more guidance on this topic.

Given the increasing prominence of the data brokerage industry which facilitates the packaging and sale of personal information, often without an individual's knowledge or consent, the Committee noted that it is important to balance the need to promote innovation while continuing to ensure that individuals have meaningful control over their personal information. Based on the prevalence of distribution of information among data brokers, it is important to ensure that such processes are clearly documented and transparent. Committee Members considered the privacy principle of "limited use," which stipulates that information should not be used for any purpose other than what it was originally collected for. Members also agreed with stakeholders that the GDPR's language of data processor and data controller better reflects the modern data economy, and the language in PIPA should be adjusted to reflect this. Data controllers should also obtain explicit consent from individuals prior to the sale of their data.

RECOMMENDATIONS

The Special Committee recommends to the Legislative Assembly that the provincial government:

15. Ensure that PIPA provides or strengthens provisions regarding access requests, including fee schedules, timeframes, applicable information, enforcement, and consequences of failing to provide access to an individual's information, whether requested by an individual or a third-party organization on behalf of an individual.
16. Allow an organization to refuse an access request when the disclosure would include the confidential information of persons fleeing or having fled domestic violence or abuse.
17. Provide individuals with the right to obtain their own personal information from an organization in a structured, commonly used, and machine-readable format at a cost no greater than the actual cost of fulfilling the access request.
18. Define the general requirements of data destruction and require organizations to clearly outline retention periods and methods of data destruction in their privacy policies.
19. Require organizations to create privacy impact assessments prior to beginning a new project that will require the processing of sensitive information with a high degree of risk to individuals and allow the OIPC to request these PIA's when necessary.
20. Allow for the collection, use, and disclosure of information without consent where a reasonable person would agree that the information is required for an investigation or prevention of fraud or criminal activity.
21. Include provisions in PIPA to ensure that data controllers are responsible for the personal information they transfer to a data processor, and that data controllers must use contractual or other means to ensure compliance with PIPA or to provide a comparable level of protection.

22. Require data controllers to obtain explicit consent from individuals prior to the sale of their data.

The Special Committee recommends to the Legislative Assembly that the Office of the Information and Privacy Commissioner:

23. Produce guidance documents on the permissibility of scanning social media profiles for information and/or provide guidance documents on the best practices for adjusting personal privacy settings and the risks associated with social media profiles and personal privacy.

EMPLOYER ACCOUNTABILITY

PIPA permits organizations to collect employee personal information without consent for the purposes of establishing, managing or terminating an employer-employee relationship. The collection must be reasonable, and the employee must be informed beforehand about the collection and purposes for the collection. Some employee protections are provided in PIPA, including Section 1, which provides a clear definition of employee personal information; Sections 13, 16, and 19 provide a right of notification if information is collected, used, or disclosed without consent; Section 32 which states that an employee cannot be charged a fee for requesting/accessing their employee personal information; and Section 54 which provides protections for employees should they complain about a privacy violation by their employer.

The Retail Action Network (RAN) noted that some smaller businesses and their employees are unaware of the rights and responsibilities as set out in PIPA, and as a result, violations often go unreported. They added that the collection of employee information varies considerably among organizations. Workers subjected to the most egregious forms of employee information collection, such as video surveillance of staff break areas, are often low wage, marginalized, and unable to allocate the time and resources necessary to file a complaint against their employer. RAN indicated that under PIPA, employees have limited rights that are under-communicated and not adequately protected, thereby setting the stage for a power imbalance between employees and employers. RAN further told the Committee that this power imbalance is not often recognized by OIPC investigators and that investigators tend to favour employers. They suggested that employers should ensure that their workers are aware of any monitoring tools and these tools should not be unduly invasive of workers' privacy.

The British Columbia Government and Service Employees' Union noted that the rapidly evolving technological environment has meant that employees are subjected to increased data collection. The Canadian Civil Liberties Association stated that the amount of employee biometric data that has been deemed reasonable to collect has increased in light of the COVID-19 pandemic. They also noted that because of limited restrictions on the collection of employee information, workers may also be subjected to surveillance in their homes, highlighting the significant risk that work productivity monitoring tools may collect information about workers' personal lives, family members, and homes, especially given that many remote workers use their own computers. They indicated that information gathered incidentally about remote workers via workplace monitoring tools should not be included in core employment decisions.

Stakeholders noted that when an individual or employee brings forward a complaint regarding an organization or their employer to the OIPC, it is the OIPC's standard practice to refer the complainant back to the organization or employer to try to resolve the issue within a 30-day period. Stakeholders, including the RAN and John Kurian, proposed this waiting period should be removed or shortened as it can lead to increased stress levels for employees who have filed a complaint.

The Chartered Professionals in Human Resources of BC and Yukon noted that PIPA appropriately acknowledges the special relationship between an employer and employee which provides an employer with broad rights to collect, use, and disclose employee personal information. They also noted that any changes to PIPA should continue to acknowledge the need for employers to have some flexibility with respect to reasonable collection of employee data, including the right for an employer to monitor social media for disparaging comments by employees. They also suggested that since PIPA came into force in 2004, employees are increasingly using their own personal devices to conduct work which heightens the risk of inadequate agreements, safeguards, or supports to ensure that personal information is properly protected. They further noted that PIPA should remedy this by outlining rules for data security for employee held information while traveling abroad and remote wipe protocols. Further the OIPC should provide

educational resources to assist employers in managing a bring-your-own-device policy.

Committee Discussion

The Committee agreed that employers do need enhanced access to employee information without consent to manage employee/employer relationships. However, Committee Members noted that during the COVID-19 pandemic, there has been an increase in the volume of information collected by employers as well as provided by employees, requiring a reexamination of the current provisions in the Act. Members noted that businesses need to be able to clearly understand their responsibilities under PIPA, and that it is equally important for employees to know what personal information is or is not permissible for an employer to collect, use and disclose.

Committee Members acknowledged that issues related to employees and workplace standards are typically within the purview of the *Employment Standards Act* (R.S.B.C. 1996, c. 19; the Committee noted however that provisions within PIPA related to employee privacy should include similar protections. In particular, the Committee wanted to ensure that there is stronger enforcement of employee privacy rights and that employers clearly display information regarding employee privacy rights in the workplace to help increase awareness and education among employees.

Members were concerned about the perceived lack of safeguards in place to guarantee that employees will not face retaliation, including termination, for bringing forward a privacy complaint to their employer or for witnessing a privacy violation or complaint. The Committee was aware that there is a provision in PIPA that allows for an individual's complaint to be dealt with directly by the OIPC if they fear retaliation by their employer, thus forgoing the 30-day resolution period; however, Members wondered if the current provisions regarding employee protections may not be clear to employers and employees and wanted to see employee protections more clearly outlined in the Act.

With the increased use of personal devices in workplaces and the increased number of employees working from home, the Committee expressed concerns that employees may be making the decision to use personal devices without an awareness of the potential consequences or risks associated with this practice. Committee Members noted that a "bring your own device" policy can result in increased collection of the employee's personal information and may also represent an increased risk to any customer information that may be on the employee's personal device.

RECOMMENDATIONS

The Special Committee recommends to the Legislative Assembly that the provincial government:

24. Strengthen existing provisions in PIPA and create a distinct section in the Act related to employee privacy including: protections for employees who make a privacy-related complaint against their employer, including job protection; limits on, and notification of, the collection of employee data; and a requirement to post information regarding employee privacy rights and employer responsibilities in workplaces. Ensure that similar protections are extended to employees and others who witness a privacy violation or complaint.

25. Revise PIPA to address the increased use of employee personal devices in the workplace, and the potential risks to information of employers, employees, customers and clients.

HEALTH INFORMATION

Medical health practitioners in British Columbia are subject to various statutory requirements under PIPA, FIPPA, PIPEDA and the *E-Health (Personal Health Information Access and Protection of Privacy) Act*, as well as other legislation which have different provisions for protecting the personal information of patients. These various provisions leave many practitioners unclear as to their responsibilities. Section 18(1) (a) and (b) of PIPA state that an organization may only disclose personal information about an individual without the consent of the individual, if (a) the disclosure is clearly in the interests of the individual and consent cannot be obtained in a timely way, or (b) the disclosure is necessary for the medical treatment of the individual and the individual does not have the legal capacity to give consent. The GDPR considers health information as "sensitive data" and therefore requires additional security measures or safeguards, including more strict requirements on the data processor and more explicit requirements for consent.

Speech and Hearing BC stated that the overlap of various legislation is unnecessarily complex and can lead to confusion among healthcare professionals regarding which legislation applies in a particular circumstance. The Canadian Bar Association, BC Branch and the Canadian Mental Health Association BC Division both echoed this comment and noted that this is further complicated by the numerous inconsistencies between FIPPA and PIPA respecting the governance of personal health information. The Canadian Bar Association, BC Branch indicated that the COVID-19 pandemic has introduced new challenges and responsibilities for the private sector with respect to collecting and processing personal health information. The BC Schizophrenia Society expressed similar concerns and indicated that a person with a mental illness could be seen one day at a mental health clinic under FIPPA rules, and the next day in a psychiatrist's private office governed by PIPA.

The Information and Privacy Commissioner for BC indicated that their office has advocated for stand-alone health information legislation and supports this initiative, noting that BC is the only province that does not have distinct legislation devoted to the privacy of health-related information and data. The Commissioner indicated that the creation of such legislation could help alleviate confusion and simplify the privacy of health information, for both medical professionals and British Columbians.

Regarding the provision of virtual health care services, the College of Physical Therapists of BC and the College of Occupational Therapists of BC noted that even before the COVID-19 pandemic, there was a shift towards the provision of telehealth services, and they noted that the pandemic had changed the way that health care services will be provided in the future. They suggested that the OIPC provide guidance and training for health care workers on the requirements for the use of technology in the delivery of health care services to ensure appropriate protection of personal privacy.

Medical Consent

The Schizophrenia Society noted that families of individuals with debilitating mental illnesses, such as schizophrenia, are often concerned that they will be unable to access confidential information in order to provide support to their family members. For example, one individual with two family members with severe mental illnesses indicated that they have been unable to effectively participate in the treatment of their family members due to provisions which limit their ability to obtain information without the consent of the individual who is ill. The Schizophrenia Society also expressed concerns about the confidentiality of the information provided to medical professionals by family members in relation to patient care. The Canadian Mental Health Association BC Branch noted that none of the exceptions to consent in PIPA relate to disclosing information about somebody experiencing a mental health episode even though such disclosure may be beneficial to the individual's health.

Also related to consent, the College of Physical Therapists and the College of Occupational Therapists of BC expressed concern about the lack of clarity around obtaining consent from children, and the legality of sharing information between medical professionals for the purposes of providing care for an individual. The Canadian Life and Health Insurance Association noted that they are required to provide medical information directly to individuals who requests this information in relation to a claim; however, they expressed concerns that the medical information provided can sometimes be distressing in nature if not appropriately explained by a medical professional.

Committee Discussion

The Committee considered the issues, concerns and confusion regarding the various statutes that relate to the provision of healthcare for British Columbians which can include care provided through e-health and telehealth initiatives. Committee Members recognized the complexity, overlap and interplay between various acts that govern healthcare data, including PIPA, FIPPA, and the *E-Health Act*, among others, noting that this can cause confusion and frustration for patients, families and healthcare providers.

Committee Members acknowledged the concerns expressed by families of individuals with mental health issues who would like to receive more information from healthcare practitioners in order to improve communication and collaborative care. Providing information to family members without an individual's consent could, in some circumstances, translate into better and more supportive care to patients. Committee Members determined that these situations would be best dealt with on a case-by-case basis.

The Committee understood the current limitations of the use of information for public health and research purposes and suggested that, with clear provisions outlining the requirements for information to be considered anonymized, there could be a range of innovative opportunities for anonymized health data to be used for public health and research purposes in the interest of improving health and wellbeing in British Columbia, across the country and internationally, while still preserving the privacy of the data subject.

Regarding perceived gaps between FIPPA and PIPA in instances where public sector organizations outsource work to private sector organizations, Committee Members expressed concerns about how such a gap might impact the flow of information between government ministries and healthcare practitioners who provide services to ministry clients which could result in an individual being required to unexpectedly pay for practitioner fees that fall outside of coverage limits.

RECOMMENDATIONS

The Special Committee recommends to the Legislative Assembly that the provincial government:

26. Create legislation dedicated to governing the collection, use and disclosure of health information in the public and private sectors.
27. Ensure that PIPA and FIPPA explicitly allow for the use of anonymized health data for public health and research purposes.
28. Harmonize PIPA and FIPPA to better facilitate sharing of personal information between government ministries and healthcare practitioners in a manner that respects the privacy rights of clients and patients.

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

The Information and Privacy Commissioner for British Columbia provides oversight and enforcement of PIPA as well as of the *Freedom of Information and Protection of Privacy Act* (FIPPA). Sections 36 of PIPA outlines the general powers of the Commissioners and Section 38 outlines the powers of Commissioner in conducting investigations, audits or inquires; Part 11 outlines how an individual might initiate a review or investigation.

GDPR Article 58 provides for the investigative, corrective and advisory powers of the supervisory authority, while Recital 122 broadly describes the scope of the supervisory authority to handle complaints and conduct investigations, as well as to promote public awareness of the risks, rules, safeguards and rights in relation to the processing of personal data.

Investigations

Section 36(1)(a) of PIPA stipulates that the Commissioner may initiate investigations and audits to ensure compliance with any provision of this Act (whether a complaint is received or not), if the Commissioner is satisfied there are reasonable grounds to believe that an organization is not complying with the Act. There are 30-day and 90-day stipulations in PIPA regarding the timeframe the Commissioner has to complete an inquiry, depending on whether or not mediation was used to settle the matter on which a complaint was based. The Commissioner may also specify a later date for completion of an inquiry.

A number of organizations and individuals proposed that the Office of the Information and Privacy Commissioner be authorized to initiate investigations more proactively and to issue orders based on these investigations. The BC Government Employee and Service Union noted that "independent investigations are important because of the increasingly complex information and data flows in today's world. Many commercial and large organizations do not process personal information in a straightforward manner, and it is simply not possible for the average person to even know that their information is improperly collected or used, let alone complain about it."

The UK Information Commissioner and former Information and Privacy Commissioner for British Columbia, Elizabeth Denham, stated that amending PIPA to allow the Commissioner to proactively initiate investigations would enable them to identify systemic issues and privacy risks and would help revamp PIPA's enforcement provisions more generally along the lines of what is stipulated in BC's FIPPA. Her view was that it was a priority that PIPA be amended to enable the Commissioner to investigate - or audit - an organization's compliance without having, as PIPA currently requires, "reasonable grounds to believe that an organization is not complying with PIPA."

Conversely, the Canadian Marketing Association indicated that they are not in favour of the Commissioner initiating investigations without the reasonable grounds provision as they noted that this level of power could further threaten the positive and constructive engagement needed between the OIPC and organizations, the majority of whom are trying to comply with the Act. Similarly, the Insurance Bureau of Canada indicated that the current model of the Commissioner initiating investigations works well and there is no need to change this.

Administrative Monetary Penalties or Fines

The Commissioner can apply to the BC Supreme Court for an order which could result in a fine. Pursuant to Section 56 of PIPA, an organization or person that commits an offence under 56(1) is liable to a fine of not more than $10,000 (individuals) or not more than $100,000 (organizations). However, there are no provisions under PIPA for the Commissioner to impose fines or administrative monetary penalties. Offences under Section 56(1) include: deception or coercion to collect personal information in contravention of the Act; disposal of personal information with an intent to evade a request for access to the personal information; obstructing the Commissioner in the performance of their duties or powers under the Act; knowingly makes a false statement to the Commissioner, or knowingly

misleading the Commissioner; contravening Section 54; or failing to comply with an order made by the Commissioner under the Act. In comparison, the GDPR stipulates that Data Protection Authorities can issue fines of up to 10 million euros or 4 percent of annual worldwide turnover, whichever is higher. Article 83 of the GDPR allows for fines to also be initiated by the supervisory authority and imposed by competent national courts in cases where the legal system of a Member State does not provide for such administrative fines.

The former Information and Privacy Commissioner for British Columbia, David Loukidelis, stated that PIPA should be amended to give the Commissioner the authority to impose administrative monetary penalties (AMPs) after a process of notice and hearing, subject to oversight through judicial review. He noted that other Commissioners in BC, such as the Chief Electoral Officer, have the power to impose monetary penalties, as does the Ontario Information and Privacy Commissioner. Mr. Loukidelis suggested that the maximum penalty should be "sufficiently high to deter serious violations of the law, but not so high as to create possible hardship for BC organizations." He also noted that the Commissioner should be required to publish a framework for administrative monetary penalties similar to what is currently included in legislation recently passed in Québec (*An Act to modernize legislative provisions as regards the protection of personal information*.) A number of organizations, including the BC Freedom of Information and Privacy Association, BC Society of Transition Houses, and the BC Civil Liberties Association stated that mandating reasonable monetary penalties for privacy violations, proportionate to the severity of the privacy issue and size of the organization, could help improve public confidence in PIPA and align BC with other more progressive legislation around the world.

In his submission to the Committee, Sean Kealy noted that "the current privacy landscape in BC is reliant on organizations choosing to follow PIPA and failure to properly comply with the legislation appears to have few consequences." In their submission to the Committee, the BC Freedom of Information and Privacy Association noted that while it is an unfortunate necessity that strong enforcement measures are needed to promote compliance, in its current form, PIPA does not contain adequate tools to ensure compliance with its requirements. Conversely, the Canadian Marketing Association and AggregateIQ stated that introducing administrative monetary penalties would undermine the collaborative relationship between the OIPC and organizations. AggregateIQ stated that PIPA does a good job of holding companies accountable and that the current system allows companies to work with the Commissioner to resolve privacy issues. Rogers Communications indicated that the current level of enforcement powers related to the Commissioner's duties and oversight are sufficient.

The Information and Privacy Commissioner for BC noted that his office has always emphasized an educational and remedial approach to compliance with PIPA; however, there are bad actors who do not wish to comply with their obligations under the Act. The Commissioner proposed a flexible system of legal enforcement to impose administrative monetary penalties on organizations that refuse to protect the personal information of British Columbians. Compliance agreements with organizations are an effective compliance tool for Commissioners that should be recognized in PIPA. The Privacy Commissioner of Canada, Daniel Therrien, noted that an effective regulator "must be properly equipped with meaningful powers that lead to quick and effective remedies." He also stated that based on the immense profits that can be made through the inappropriate use of personal data, serious financial penalties are imperative and there needs to be real consequences for businesses that break the law, along with incentives to comply. The Commissioner would also like to be able to share information with international privacy regulators to support complex investigations. TECHNATION suggested that the current structure of the OIPC could be split into two separate arms; one with investigative responsibilities and the other responsible for issuing orders and making decisions regarding administrative monetary penalties (if implemented).

Accessibility, Transparency and Education

The BC Freedom of Information and Privacy Association indicated that in their 2020 survey of British Columbians, less than half of respondents were aware of PIPA; the Office of the Information and Privacy Commissioner; the ability to make complaints; or the ability to request access to their personal information. Some organizations, such as Chartered Professionals in Human Resources of BC and Block Watch Society of BC indicated that the OIPC could improve the accessibility and transparency of their work, as well as provide increased public education to raise awareness of the OIPC's mandate, services, and resources.

The Pacific Legal Education and Outreach Society and the BC Society of Transition Houses outlined the specific needs of non-profit organizations and how the OIPC could provide further education, training and awareness regarding how to ensure these organizations comply with PIPA and share best

practices for handling and protecting personal information. The Society also proposed that additional funding be provided to non-profit organizations so they can learn how to draft privacy impact assessments to more effectively manage the personal information of individuals who access their services.

Registry and Accreditation of Privacy Professionals

While many companies have a dedicated privacy officer or other individual responsible for privacy policies and administration, a number of organizations, including the Chartered Professionals in Human Resources of BC, suggested that professional accreditation and/or a registry of privacy professionals could help provide privacy officers with both the knowledge and means by which they can ensure that their organization's privacy policies and practices adequately comply with PIPA.

The Chartered Professionals in Human Resources of BC suggested that an accreditation or certification program should be created for organizations and privacy officers based on internationally accepted privacy standards for organizations to develop their knowledge of privacy standards and best practices to help improve their privacy practices and raise public awareness.

Committee Discussion

The Committee discussed the input received regarding the Commissioner's powers, and the need to strengthen them so that the Commissioner is able to identify and investigate broader systemic issues. Committee Members also considered the concerns of some stakeholders that this could negatively affect the collaborative and constructive relationship between the OIPC and organizations. The Members noted that some data regulators in other jurisdictions already have these enhanced powers. Committee Members indicated that it would be beneficial for the Commissioner to be able to conduct audits with the goal of identifying and investigating systemic issues and to have the ability to issue findings and orders in relation to these audits.

Committee Members considered provisions in provincial and international legislation in relation to administrative monetary penalties (AMPs) or fines associated with regulators' enforcement of the provisions within privacy legislation. Members agreed that the Commissioner should be empowered to assess and issue fines directly and discussed input which suggested that administrative monetary penalties need to be significant enough to act as a deterrent to bad actors and criminals who willfully violate the Act. They also highlighted the need to consider the severity of the violation, the incident's impact on the privacy of individuals, and the impact of significant fines on a small business or non-profit organization. The Committee indicated that proportionality and scalability also need to be key factors in determining fines or penalties and wanted to ensure that AMPs are proportional with other jurisdictions and reflective of British Columbia's share of the global market. However, Committee Members had diverging views regarding the amount of the fines. Some Members felt that the level of penalties should be updated to account for inflation; others, that it should be reflective of British Columbia's share of the global market; still others proposed that the amount of the fines currently prescribed in Section 56 be increased to align more closely with the GDPR.

The Committee noted that the Commissioner has highlighted the importance of a collaborative relationship with businesses in BC and that the initial approach of his office is always educational and preventative in nature to provide the opportunity for organizations to resolve issues on their own and reserve the application of AMPs for the most serious offences or issues.

The Committee expressed appreciation for the OIPC's efforts to educate British Columbians and raise awareness of PIPA through its communications, guidance documents and other outreach initiatives. However, Members expressed concerns about the lack of public awareness of the Act and noted that British Columbians cannot effectively protect their personal information or defend their privacy rights if they are not aware of the provisions of PIPA. More needs to be done to increase public knowledge of the Act and Members would like to see the OIPC increase its education and awareness efforts. In particular, Committee Members wanted to see more resources made available to small and medium sized businesses and non-profits to help increase their knowledge of the Act and provide information on the best ways to collect, use and safeguard the personal information of customers and clients, including basic how-to resources, such as a "PIPA 101" offering.

RECOMMENDATIONS

The Special Committee recommends to the Legislative Assembly that the provincial government:

29. Include provisions in PIPA to enhance the Commissioner's ability to conduct audits to identify and investigate systemic issues, as well as to issue findings and orders where there are reasonable grounds to do so.

30. Include provisions in PIPA to strengthen the Commissioner's power to enforce PIPA and expand audits of private sector organizations; enter into compliance agreements with organizations; and require organizations to produce relevant reports upon request.

31. Ensure that PIPA includes provisions to grant the Commissioner the power to levy administrative monetary penalties currently found under the Act against organizations found to be in violation of PIPA proportional to the severity of the violation.

32. Ensure that administrative monetary penalties are set at an amount that is a sufficient deterrent to contraventions of the Act.

The Special Committee recommends to the Legislative Assembly that the Office of the Information and Privacy Commissioner:

33. Expand the OIPC's public education initiatives, including raising awareness of the Act through increased communications and resource materials, and with additional supports or resources focused on small businesses and non-profit organizations.

PIPA INTERPLAY WITH OTHER LEGISLATION

A number of other statutes were identified during the course of the consultation due to a perceived overlap or confusion with provisions within PIPA, or due to apparent gaps between PIPA and other legislation. These include the *Strata Property Act*, *Societies Act*, *Land Owner Transparency Act*, and the *Canadian Charter of Rights and Freedoms*.

Strata Property Act

Section 18(1)(o) of PIPA states that an organization may disclose personal information without the consent of an individual if the disclosure is required or authorized by law. Section 36 of the *Strata Property Act* (S.B.C. 1998, c. 43) (SPA) requires strata corporations to produce records or documents requested by a strata resident or owner within two weeks of receiving the request. The Commissioner informed the Committee that the OIPC issued guidance documents on the intersection of these two laws in 2009 and again in 2015. According to the Commissioner's 2015 guidelines, Section 135 of the SPA authorizes the disclosure of the particulars of a complaint; however, it stipulates that "the disclosure should not exceed that which a reasonable person would consider appropriate in the circumstances." The guidelines also stipulate that "while in most circumstances it would not be appropriate to disclose the identity or strata lot of the complainant, there may be circumstances where that information is so inextricably linked to the complaint that the disclosure would be reasonable."

The guidelines further explain that "the requirement to provide access to correspondence found in Sections 35 and 36 of the SPA is clear and any personal information in that correspondence need not be withheld under PIPA" and provides further clarification by adding that "while the disclosure of personal information in the particulars of a complaint should be limited as described above, this does not mean that correspondence required to be provided under Section 36 of the SPA is to be limited or severed in any way under PIPA, even where that correspondence relates to a complaint."

Based on the issues raised regarding the interplay between the SPA and PIPA, the Committee requested a briefing from the Ministry of Municipal Affairs and Housing and Doug Page, Director of Policy and Legislation with the Housing Policy Branch presented to the Committee on September 16, 2020. Mr. Page noted that strata corporations are sometimes seen as a "fourth level" of government, as they have the ability to issue fines, collect payments in the form of strata fees, make bylaws, and elect councils. As a result of these activities, strata corporations may collect sensitive personal information. There is some disagreement with the Commissioner's interpretation of PIPA in the 2015 guidance document, and the issues appear to have escalated. Mr. Page also remarked that if PIPA does not apply to Sections 36 and 135 of the SPA, then a privacy gap exists as there would be no statutory grounds to withhold personal information. He further noted that transparency is important for strata corporations to remain accountable and to ensure good governance, and he believes a balanced resolution can be found.

The Condominium Home Owners' Association raised concerns regarding the 2015 guidance document issued by the Commissioner and noted that it could potentially permit the release of sensitive personal information, including health or financial details. On the other hand, some stakeholders expressed concerns that amending the SPA to protect the private records of tenants may be used by strata corporations to justify withholding important documents. During his September 16, 2020 presentation to the Committee, the Commissioner indicated that the SPA, not PIPA, requires amendments to balance the information and privacy needs of condominium owners with appropriate privacy protections. He suggested that, prior to any amendments to the SPA, an in-depth policy and legal review take place to consider the complexity of the privacy requirements under consideration and any potential impacts.

Societies Act

In their presentation to the Committee, the Alma Mater Society at UBC Vancouver indicated that under the *Societies Act* (S.B.C. 2015, c. 18), their organization is responsible for maintaining a register of its members. The Society expressed concerns that previously, this information would be disclosed by the university; however, recently, the university has stopped sharing this information due to privacy concerns. The society noted that Section 12(2) of PIPA allows for the disclosure of information between organizations without the consent of the individual if the personal information is disclosed to or collected by the organization solely for the purposes for which the information was previously collected, and to assist that organization to carry out work on behalf of the other organization. They further noted that there currently is no provision that allows for similar collection from a public body under FIPPA such as a university or college; and they stated that this absence limits their functionality. The Society suggested that PIPA be amended to ensure that student societies are able to obtain lists of their members from a public body and specifically to amend Section 12(2) to allow student societies to collect personal information from the university or college without the consent of the student. The proposed amendment should specify that personal information may be collected by a student society from a public body in order for the student society to conduct elections, contact its members and conduct other routine business.

Solicitor-client Privilege

The Law Society of BC raised concerns with respect to PIPA's potential impact on solicitor-client privilege and noted that Section 3(3) of PIPA states that "nothing in this Act affects solicitor-client privilege." However, Section 38(5) of PIPA states that any evidence requested by the Commissioner must be turned over, regardless of any legal privileges. The Law Society of BC and the Canadian Bar Association, BC Branch, highlighted the potential conflict between these provisions in PIPA, and emphasized that the right of solicitor-client privilege and claims of privilege should be adjudicated by a judge, not by the Commissioner.

Other Legislation

The British Columbia Real Estate Association indicated that realtors deal with sensitive personal information and need legislation which provides certainty and addresses modern technologies and business practices. While they support government efforts to limit money laundering, they warned that tools such as the *Land Owner Transparency Act* (S.B.C. 2019, c. 23) and associated registry, as well as the beneficial ownership registry, could make significant amounts of information public.

In their submission to the Committee, the Watch Tower Bible and Tract Society of Canada indicated that by interfering with the creation and preservation of confidential religious information, PIPA unjustifiably violates the fundamental rights and freedoms of congregation elders and fellow Jehovah's Witnesses protected by the *Canadian Charter of Rights and Freedoms*. They noted that the lack of exemptions in PIPA for religious ministers and religious congregations seriously compromises the ability of elders in British Columbia to provide effective pastoral support.

Committee Discussion

Committee Members discussed the issue raised by the Condominium Homeowners Association and other stakeholders regarding the potential conflict or confusion in relation to the disclosure requirements outlined in PIPA and the *Strata Property Act* (SPA). The Committee agreed with the Information and Privacy Commissioner who suggested that the issue might be dealt with through amendments to the SPA, rather than PIPA. Similarly, regarding the information brought forward to them from the Alma Mater Society of UBC Vancouver, Committee Members expressed concerns about amending the relevant section in PIPA as was suggested by the Society and indicated that the issue might be more appropriately dealt with internally between the two organizations through a Memorandum of Understanding or through a revision to student forms to provide for explicit consent to share information with the Society. Additionally, Members discussed the input brought forward by The Law Society of BC and the Canadian Bar Association, BC Branch regarding solicitor-client privilege and the current provisions in PIPA that relate to this issue; however, the Committee noted that these issues had been recently dealt with by the Supreme Court of Canada, in *Alberta (Information and Privacy Commissioner) v University of Calgary*, 2016 SCC 53 [Alberta], where the Supreme Court of Canada clarified solicitor-client privilege in the context of privacy legislation.

RECOMMENDATION

The Special Committee recommends to the Legislative Assembly that the provincial government:

34. Undertake a review of the *Strata Property Act* (SPA) to resolve issues related to potential conflict or confusion regarding the disclosure requirements outlined in PIPA and SPA.

STATUTORY REVIEW

As noted, Section 59 of PIPA stipulates that a special committee of the Legislative Assembly must undertake a comprehensive review of the Act every six years, which is the same review period stipulated in BC's *Freedom of Information and Protection of Privacy Act*. In comparison, the GDPR is reviewed every four years and PIPEDA is reviewed every five years.

In their 2021 submission, ISACA Vancouver Chapter advocated for a more frequent review of PIPA and that a panel of organizations could be established to offer ongoing input to the Committee between reviews to ensure that PIPA is informed by the most current information about digital business models and any changes to how personal data is handled globally. Similarly, Em Hunter indicated that more frequent reviews of the Act might help keep pace with a rapidly changing privacy environment.

Committee Discussion

In light of changes to privacy, the protection of personal data and the rapid development and adoption of new technologies, Committee Members agreed that PIPA may need to undergo a statutory review more often than every six years. However, the Committee decided not to make a recommendation at this time in light of the magnitude of the proposed recommendations outlined in the Committee's report which, if implemented, represent a significant overhaul of the legislation. Committee Members suggested that government may consider undertaking an environmental scan of the privacy landscape as necessary to complement and inform the ongoing statutory review process and to ensure that PIPA remains relevant and reflective of the current privacy landscape.

FULL LIST OF COMMITTEE RECOMMENDATIONS

Alignment and Harmonization with Other Privacy Legislation

The Special Committee recommends to the Legislative Assembly that the provincial government:

1. Ensure that PIPA meets GDPR and anticipated federal adequacy requirements.
2. Update PIPA with a focus on prioritizing interoperability with other provincial and interna-tional legislation, including the GDPR.

New and Emerging Technologies

The Special Committee recommends to the Legislative Assembly that the provincial government:

3. Ensure that PIPA include definitions of pseudonymized information as personal information, and anonymized information as outside the scope of PIPA, similar to definitions in the GDPR.
4. Ensure PIPA prohibits the reidentification of pseudonymized or anonymized information by any person, organization, or contractor other than the originally authorized person, organization, or contractor.
5. Ensure that PIPA requires an organization to notify an individual that automated processes were used to make a significant decision about them and includes provisions to allow an individual to request human intervention in the decisionmaking process.
6. Require organizations to reaffirm the consent of individuals to collect, use, disclose, or process biometric data with reasonable frequency.
7. Explicitly require an organization to delete biometric information within a reasonable timeframe upon the request of an individual.

The Special Committee recommends to the Legislative Assembly that the Office of the Information and Privacy Commissioner:

8. Undertake a public consultation to study the long-term socioeconomic impacts of artificial intelligence, including automated decision making and automated profiling, and provide the Ministry of Citizens' Services with any recommendations for proposed amendments to the Act.

Meaningful Consent

The Special Committee recommends to the Legislative Assembly that the provincial government:

9. Update the requirements of explicit consent to include meaningful consent provisions.
10. Align the exemptions to consent in PIPA with those of the GDPR.
11. Define new sensitive categories of information in PIPA which would require explicit consent from individuals and specific data handling practices to include: biometric data, political views, religion, sexual orientation, medical information, and information related to children and youth.

The Special Committee recommends to the Legislative Assembly that the Office of the Information and Privacy Commissioner:

12. Develop guidance information explaining the importance and benefits of the principles of "privacy by design."

Mandatory Breach Notification

The Special Committee recommends to the Legislative Assembly that the provincial government:

13. Include provisions in PIPA similar to those in other jurisdictions to require organizations to promptly notify the OIPC and affected individuals of a privacy breach, with consideration for proportionality regarding the severity of the breach.

14. Ensure that PIPA allows for various direct methods of communication to notify affected individuals of a breach, including email, text, phone call or regular mail.

Disclosure of Personal Information

The Special Committee recommends to the Legislative Assembly that the provincial government:

15. Ensure that PIPA provides or strengthens provisions regarding access requests, including fee schedules, timeframes, applicable information, enforcement, and consequences of failing to provide access to an individual's information, whether requested by an individual or a third-party organization on behalf of an individual.

16. Allow an organization to refuse an access request when the disclosure would include the confidential information of persons fleeing or having fled domestic violence or abuse.

17. Provide individuals with the right to obtain their own personal information from an organization in a structured, commonly used, and machine-readable format at a cost no greater than the actual cost of fulfilling the access request.

18. Define the general requirements of data destruction and require organizations to clearly outline retention periods and methods of data destruction in their privacy policies.

19. Require organizations to create privacy impact assessments prior to beginning a new project that will require the processing of sensitive information with a high degree of risk to individuals and allow the OIPC to request these PIA's when necessary.

20. Allow for the collection, use, and disclosure of information without consent where a reasonable person would agree that the information is required for an investigation or prevention of fraud or criminal activity.

21. Include provisions in PIPA to ensure that data controllers are responsible for the personal information they transfer to a data processor, and that data controllers must use contractual or other means to ensure compliance with PIPA or to provide a comparable level of protection.

22. Require data controllers to obtain explicit consent from individuals prior to the sale of their data.

The Special Committee recommends to the Legislative Assembly that the Office of the Information and Privacy Commissioner:

23. Produce guidance documents on the permissibility of scanning social media profiles for information and/or provide guidance documents on the best practices for adjusting personal privacy settings and the risks associated with social media profiles and personal privacy.

Employer Accountability

The Special Committee recommends to the Legislative Assembly that the provincial government:

24. Strengthen existing provisions in PIPA and create a distinct section in the Act related to employee privacy including: protections for employees who make a privacyrelated complaint against their employer, including job protection; limits on, and notification of, the collection of employee data; and a requirement to post information regarding employee privacy rights and employer responsibilities in workplaces. Ensure that similar protections are extended to employees and others who witness a privacy violation or complaint.

25. Revise PIPA to address the increased use of employee personal devices in the workplace, and the potential risks to information of employers, employees, customers and clients.

Health Information

The Special Committee recommends to the Legislative Assembly that the provincial government:

26. Create legislation dedicated to governing the collection, use and disclosure of health information in the public and private sectors.

27. Ensure that PIPA and FIPPA explicitly allow for the use of anonymized health data for public health and research purposes.

28. Harmonize PIPA and FIPPA to better facilitate sharing of personal information between government ministries and healthcare practitioners in a manner that respects the privacy rights of clients and patients.

Office of the Information and Privacy Commissioner

The Special Committee recommends to the Legislative Assembly that the provincial government:

29. Include provisions in PIPA to enhance the Commissioner's ability to conduct audits to identify and investigate systemic issues, as well as to issue findings and orders where there are reasonable grounds to do so.

30. Include provisions in PIPA to strengthen the Commissioner's power to enforce PIPA and expand audits of private sector organizations; enter into compliance agreements with organizations; and require organizations to produce relevant reports upon request.

31. Ensure that PIPA includes provisions to grant the Commissioner the power to levy administrative monetary penalties currently found under the Act against organizations found to be in violation of PIPA proportional to the severity of the violation.

32. Ensure that administrative monetary penalties are set at an amount that is a sufficient deterrent to contraventions of the Act.

The Special Committee recommends to the Legislative Assembly that the Office of the Information and Privacy Commissioner:

33. Expand the OIPC's public education initiatives, including raising awareness of the Act through increased communications and resource materials, and with additional supports or resources focused on small businesses and non-profit organizations.

PIPA Interplay with Other Legislation

The Special Committee recommends to the Legislative Assembly that the provincial government:

34. Undertake a review of the Strata Property Act (SPA) to resolve issues related to potential conflict or confusion regarding the disclosure requirements outlined in PIPA and SPA.

APPENDIX A: PUBLIC HEARING PARTICIPANTS

AggregateIQ, Jeff Silvester (16-Jun-20, virtual)

Alma Mater Society of the University of British Columbia, Sheldon Goldfarb, Saad Shoaib (23-Jun-21, virtual)

BC Civil Liberties Association, Aisha Weaver (16-Jun-20, virtual)

BC Freedom of Information and Privacy Association, Jason Woywada (09-Jun-20, virtual)

BC Government and Service Employees' Union, Stefanie Ratjen (16-Jun-20, virtual)

BC Society of Transition Houses, Amy FitzGerald (22-Jun-21, virtual)

BC Tech Association, Jill Tipping (08-Jul-20, virtual; 07-Jul-21, virtual)

Dr. Colin Bennett (09-Jun-20, virtual, 06-Jul-21, virtual)

Block Watch Society of BC, Gabriel Pelletier (17-Jun-20, virtual)

Jade Buchanan (17-Jun-20, virtual)

Canada's Digital Technology Supercluster, Sue Paish (08-Jul-20, virtual)

Canadian Bar Association, BC Branch, FOI and Privacy Law Section, Sinziana Gutiu, Kelly Samuels (16-Jun-20, virtual)

Canadian Civil Liberties Association, Brenda McPhail (07-Jul-21, virtual)

Canadian Life and Health Insurance Association, Anny Duval, Stephen Frank (06-Jul-21, virtual)

Canadian Mental Health Association, Jonathan Morris (07-Jul-21, virtual)

Chartered Professionals in Human Resources of BC, Anthony Ariganello, Zelda Craig, Kristi Searle (17-Jun-20, virtual)

Dr. Andrew Clement (07-Jul-21, virtual)

Condominium Home Owners Association of BC, Allyson Baker, Tony Gioventu (09-Jun-20, virtual)

Digital Discretion, Stephanie Perrin (09-Jun-20, virtual)

Donald R. McLeod Law Corp., Donald McLeod (17-Jun-20, virtual; 23-Jun-21, virtual)

Dr. Mike Figurski (22-Jun-21, virtual)

Global Automakers of Canada, David Adams (22-Jun-21, virtual)

Kevin Gooden (06-Jul-21, virtual)

Information Commissioner's Office (UK), Elizabeth Denham (17-Jun-20, virtual)

Information Systems Audit and Control Association (ISACA), Anthony Green (07-Jul-21, virtual)

IPP Consulting, Marilyn Sing (09-Jun-20, virtual)

MediaSmarts, Dr. Kara Brisson-Boivin, Matthew Johnson (16-Jun-20, virtual)

Diane Milne (23-Jun-21, virtual)

Ministry of Citizens' Services, Kerry Pridmore, Matt Reed (02-Jun-20, virtual; 16-Sep-20, virtual; 23-Feb-21, virtual)

Ministry of Municipal Affairs and Housing, Doug Page (16-Sep-20, virtual)

Mortgage Brokers Institute for British Columbia and the Canadian Mortgage Brokers Association-British Columbia, Samantha Gale (22-Jun-21, virtual)

Office of the Information and Privacy Commissioner for British Columbia, Michael McEvoy, oline Twiss, Jeannette Van Den Bulk (02-Jun-20, virtual)

Office of the Information and Privacy Commissioner for British Columbia, Michael McEvoy, Michelle Mitchell, oline Twiss, Jeannette Van Den Bulk (16-Sep-20, virtual; 23-Feb-21, virtual)

Office of the Privacy Commissioner of Canada, Daniel Therrien, Brent Homan (22-Jun-21, virtual)

Pacific Legal Education and Outreach Society, Martha Rans (23-Jun-21, virtual)

Quay Pacific Property Management, Professional Association of Managing Agents, Leslie Haycock (16-Jun-20, virtual)

Gary Raddysh (09-Jun-20, virtual)

Retail Action Network, Pamela Charron, Katilyn Matulewicz, Andreea Micu (16-Jun-20, virtual)

Dr. Teresa Scassa (06-Jul-21, virtual)

Speech and Hearing BC, Anna Kruger (09-Jun-20, virtual)

Stergios Vlioras (07-Jul-21, virtual)

Wing-Sze Yung (06-Jul-21, virtual)

Gordon Yusko (07-Jul-21, virtual)

APPENDIX B: WRITTEN SUBMISSIONS

BC Green Party
BC NDP
Deanna Breuker
British Columbia Civil Liberties Association and BC Freedom of Information and Privacy Association Joint Submission
British Columbia Dental Association
British Columbia Real Estate Association
British Columbia Schizophrenia Society
British Columbia Teachers' Federation
Business Council of British Columbia
Canadian Bankers Association
Canadian Council of Innovators
Canadian Marketing Association (CMA)
Canadian Medical Protective Association
Canadian Vehicle Manufacturers' Association
Canadian Wireless Telecommunications Association
Centre for Digital Rights
College of Physical Therapists of BC and the College of Occupational Therapists of BC
Annette Denk
Vincent Gogolek
Brian Gordon
Health Sciences Association of BC
Em Hunter
Dr. Jay Fedorak
Insurance Bureau of Canada
i-SIGMA
Linda Jackson
Sean Kealy
John Kurian
LandlordBC
Law Society of BC
Ian Linkletter
Valerie Lipton
David Loukidelis, Q.C.
Wayne Masters
Tess McMechan
Bryan Melnyk
Office of the Information and Privacy Commissioner for British Columbia
Office of the Information and Privacy Commissioner of Alberta
Office of the Information and Privacy Commissioner of Ontario
Pacific Blue Cross
Dimitri Panagopoulos
Portfolio Management Association of Canada
Office of the Privacy Commissioner of Canada
Retail Council of Canada
Rogers Communications
Carol Ross
Gary Rupert
Matthew Schellenberg
Kathy Sperling
TECHNATION
Tekhnos Law
Trans Union of Canada, Inc.
VGH & UBC Hospital Foundation
Watch Tower Bible and Tract Society of Canada
West Point Grey Academy
Dylan Williams
Becky Wong