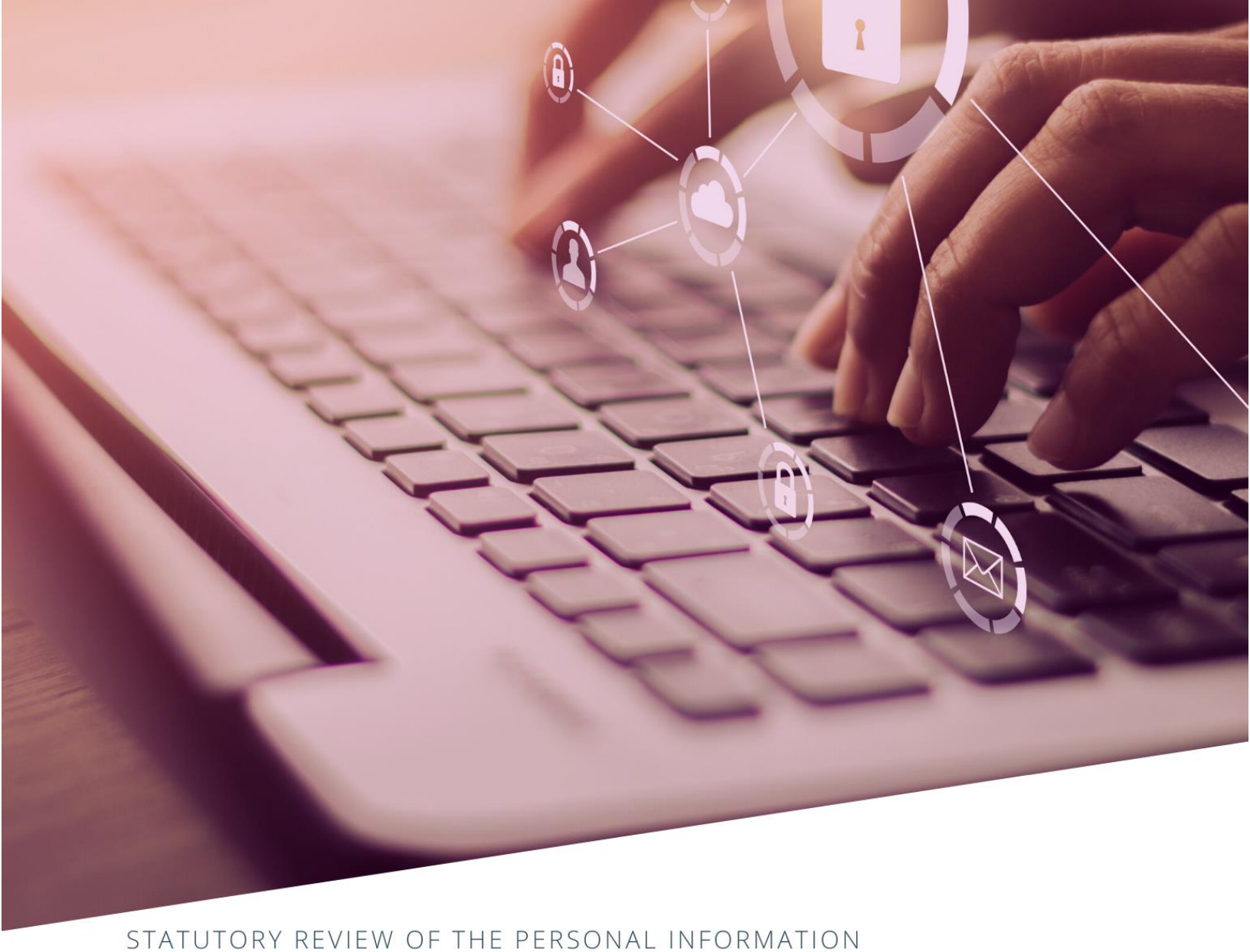

STATUTORY REVIEW OF THE PERSONAL INFORMATION PROTECTION ACT

Submission to the Special Committee to Review the Personal Information Protection Act

SEPTEMBER 16, 2020
CANLII CITE: 2020 BCIPC 47
QUICKLAW CITE: [2020] B.C.I.P.C.D. NO. 47

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

TABLE OF CONTENTS

COMMISSIONER'S MESSAGE

This is the third time my office has participated in a statutory review of PIPA since its inception 20 years ago. Although the two previous reviews led to some very sound recommendations, government's persistent failure to act has left previous Special Committees' efforts lying dormant.

Further inaction is not a viable option. PIPA's entire relevance is now at stake. British Columbia is being left behind as legislators across the country and around the world modernize their privacy laws to respond to our shift to digital economies, and to meet the challenges posed by new technologies such as artificial intelligence, data analytics, facial recognition, social media and more. Legislatures in Alberta, Quebec and Ottawa have responded. Legislatures in Europe, the United Kingdom, the United States, Japan, Korea, Brazil and elsewhere have acted. It is time for action in British Columbia.

The implications of ongoing failure to act in British Columbia extend beyond risks to privacy. Ensuring PIPA continues to give British Columbians robust yet balanced privacy protections is the right thing to do. It is also the right thing to do to help ensure that British Columbia's digital economy continues to thrive. Digital economic activities depend on the trust and confidence of businesses and citizens alike in British Columbia's privacy framework. Yet, as illustrated in this submission, across a range of issues PIPA is at serious risk of not being fit for that purpose.

The wide range of submissions received by the Special Committee reveal a broad consensus on the core enhancements necessary to modernize the law. The focus of my submission is on critically important amendments that would substantially improve PIPA's efficacy. My focus is on updating the control British Columbians have over their own personal information, increasing transparency about how organizations use our personal information, improving accountability by enhancing enforcement tools, and streamlining my office's investigation and audit powers.

It is an honour to submit these recommendations to you. Your work on this review and the recommendations you make will, I am confident, have an important and enduring impact on British Columbia's citizens and organizations.

September 16, 2020

Michael McEvoy
Information and Privacy Commissioner
for British Columbia

INTRODUCTION

This submission urges the Special Committee to recommend long overdue, critically important, enhancements to British Columbia' *Personal Information Protection Act* (PIPA). As PIPA itself illustrates, legislators have long recognized the importance of protecting citizens' privacy. PIPA was drafted almost twenty years ago, under radically different circumstances, and the challenges to privacy in our digital age threaten PIPA's relevance and its effectiveness.

Rapidly evolving technologies enable the collection of ever greater amounts of often sensitive personal information, the sophisticated profiling of individuals, indiscriminate sharing of personal information, and the permanent storage of massive amounts of our personal information at diminishing cost. Challenges also arise from private sector activities that use technologies in new ways that can create unprecedented privacy risks.

Social media platforms offer an example of the power of digital technologies to affect our privacy. There is intense and lucrative demand for the large "honeypots" of personal information held by social media giants such as Facebook, Google, Instagram and YouTube. Many businesses use our information for commercial purposes, but there is often no meaningful transparency about what elements of individuals' personal information are being collected, how the personal information is used, to whom it is disclosed, and for what purposes. Incomprehensible and one-sided privacy policies risk making a mockery of PIPA's core principle of individual consent.[1] This is only one of the ways in which the current and evolving environment challenges PIPA's ongoing fitness for purpose.

Why does it matter if PIPA is up to the task? It matters, of course, because citizens expect the government to protect privacy, which has constitutional dimensions, through meaningful legislated protections. The public opinion survey recently conducted by the BC Freedom of Information and Privacy Association—which is referred to in its submission to you—affirms that meaningful privacy protections matter to British Columbians.

Privacy also matters to digital economic activities in British Columbia; PIPA is a key part of the regulatory framework necessary for digital economies to flourish. Modern technologies and digital economic activities come with risks, but they also offer great opportunities. As Canada's Digital Supercluster notes in its submission to you:

> Digital innovation is key to economic prosperity in our province and country. Appropriately managing the balance between economic opportunity and privacy/security is essential to our future.[2]

[1] Obscurity about organizations' security measures also makes it next to impossible for the average person to assess whether proper security measures exist to protect their personal information.
[2] Page 1.

Digital economic activities are important for British Columbia. In 2017, "digital economic activities accounted for the largest share of total economic activities in Ontario, Quebec and British Columbia", with British Columbia's increase of 49.1% in digital economy jobs from 2010 to 2017 being the largest in Canada.[3] In 2017, British Columbia's technology sector revenues, at $15.7 billion annually, accounted for 7% of our GDP and the sector employed 114,000 people, or 5.2% of the workforce.[4]

The most recent figures are almost surely higher, underscoring the increasing importance of digital economic activities to British Columbia's overall economic health. The provincial and federal governments continue to actively promote and support digital economic development, with a range of programs, funding and research supports being available.

Furthermore, a digital economy can only flourish if individuals trust that their personal information will be collected, used, and disclosed within a framework of robust yet balanced privacy protections. If individuals lose confidence that their privacy will be meaningfully protected, they may well no longer allow their information to be used or be reluctant to utilize digital services. This is not conducive to a thriving, growing digital economy and is the reason many digital businesses support modern privacy laws that strike the right balance between facilitating use of digital technologies and protecting privacy.[5] As Canada's Digital Supercluster has submitted:

> Companies must be confident that our laws provide a clear and practical approach to privacy and the securing, protection and handling of data. Individuals, organizations and the state should all feel safe in the knowledge that their rights and interests are protected.[6]

Similarly, many governments recognize that a sound framework for digital economic development must include modern privacy rules, to maintain individuals' trust in digital technologies. The European Union demonstrated this through its 2018 *General Data Protection Regulation* (GDPR). California has enacted the *California Consumer Privacy Act of 2018* (California Act). The federal private sector privacy law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), has been amended and further changes appear likely. Earlier this summer Quebec introduced significant amendments to its private sector privacy law, to update it for the digital age by introducing several modern concepts from the GDPR.[7] Ontario has started a public consultation on a modern private sector privacy law for Ontario.

---

[3] Statistics Canada, "Measuring digital economic activities in Canada, 2010 to 2017". Accessed August 21, 2020.
[4] Innovate BC, "2020/21 – 2022/23 Service Plan", page 6. https://innovatebc.ca/wp-content/uploads/2020/02/Innovate-BC-Service-Plan-1.pdf. Accessed August 21, 2020.
[5] For example, Mark Zuckerberg, Facebook's head, has publicly stated his support for privacy laws that apply to his company.
[6] Page 2.
[7] Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information* [Quebec Bill 64]. http://m.assnat.qc.ca/en/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html. Accessed August 21, 2020.

Other considerations also underscore the urgency of significant improvements to PIPA. PIPA's status in relation to PIPEDA could be jeopardized if PIPA is no longer substantially similar with PIPEDA. The federal cabinet has declared PIPA to be substantially similar, but that status is increasingly at risk every time PIPEDA is modernized and PIPA is not. British Columbia's digital sector could find itself at a significant disadvantage if BC's private sector privacy laws continue to fall behind.

The above factors underpin my recommendations and the many other submissions made by business and civil liberties groups alike. Individuals and organizations across BC will benefit from modernizing PIPA for the digital economy.

The recommendations below aim to achieve this vital objective. They are grouped into four categories: privacy obligations of organizations, privacy rights of individuals, Commissioner oversight powers, and other amendments. These are the minimum necessary reforms if PIPA is to keep pace with public expectations and evolving technologies, and to foster British Columbia's economic future.

A HEALTH PRIVACY LAW FOR BRITISH COLUMBIA

It is important to mention a previous Special Committee recommendation before discussing specific PIPA reforms. The last Special Committee to review PIPA recommended enactment of a standalone health information privacy law. This would be a welcome development for many reasons.[8] It would also align British Columbia with other Canadian jurisdictions, all but one of which already have health privacy laws.

Enactment of a health privacy law would likely require consequential amendments to PIPA—and to the *Freedom of Information and Protection of Privacy Act* (FIPPA), for that matter—to ensure that the laws dovetail appropriately. The prospect that a health privacy law might be enacted someday soon must not, however, delay the PIPA reforms that are needed today.

PRIVACY OBLIGATIONS OF ORGANIZATIONS

Mandatory breach notification

After Quebec Bill 64 is enacted, PIPA will be the only Canadian general private sector privacy law that does not require organizations to, in appropriate circumstances, notify individuals whose personal information has been compromised by a privacy breach. Mandatory breach notification is already required across Europe, the UK, and the United States.

Now an outlier both domestically and internationally, PIPA fails to afford British Columbians the protections they deserve.

[8] Recommendation 14.

A significant number of organizations made submissions to you supporting mandatory breach notification. They include groups such as the Insurance Bureau of Canada, Canadian Marketing Association, Canadian Medical Protective Association, and BC Real Estate Association. My federal colleague and colleagues from Alberta, Ontario and the UK are supportive. Civil society groups such as the BC Freedom of Information Association, BC Civil Liberties Association, and other groups such as the BC NDP and the BC Government Employees' Union are also supportive. A similarly broadly-based consensus for breach notification emerged in the 2014 review of PIPA.[9]

Introducing mandatory breach notification for British Columbia is especially important now because, as we have seen, modern technologies and business practices are leading to the compilation of ever-increasing amounts of often very sensitive personal information about us. This can include personal health information, information about ethnicity or race, information about opinions or political views, or financial, educational and employment information. The information about us can include the products of artificial intelligence or other data analytics, including very sensitive profiles of our behavior and preferences.

Privacy breaches can have very serious consequences. These range from the financial harm to individuals flowing from the fraudulent misuse of someone's banking details to threats to personal safety when information about a vulnerable person's whereabouts is compromised. These are only two examples of the many kinds of harm to which individuals can be exposed where their personal information is compromised due to carelessness or wrongdoing.

Mandatory breach notification is universally recognized as having at least three main benefits.

First, it permits individuals who are notified about a breach to take steps to protect their interests. Steps can include monitoring personal financial accounts and credit history, cancelling credit cards, and changing passwords for various personal accounts.

Second, mandatory breach notification gives organizations a real incentive to invest in information security technologies and policies, to better protect personal information against compromise.[10] The impact of this key incentive is clearly underscored by Elizabeth Denham, the UK's Information Commissioner, in her submission to you.

Third, mandatory breach notification can help a regulator keep up to date on trends in risks to the security of personal information. As Jill Clayton, the Information and Privacy Commissioner of Alberta, notes in her submission, over the last decade her office has received some 1,550

[9] Breach notification was supported in 2014 by the BC Civil Liberties Association, the BC Freedom of Information and Privacy Association, the Canadian Bankers Association, the Canadian Bar Association, the Canadian Life and Health Insurance Association, the Canadian Medical Protection Association, Central 1 Credit Union and the Privacy Commissioner of Canada.

[10] This incentive can be especially powerful where, as is recommended below, organizations are subject to potentially significant sanctions for failing to respect their obligations to protect personal information.

breach notification reports from a wide range of domestic and international organizations. The Alberta Commissioner has told me that the information in these reports has helped inform her awareness of trends in privacy breaches. This has, in turn, assisted her with publishing up-to-date information and guidance for organizations and individuals about the risks to personal information.

Before articulating with more precision how mandatory breach notification should be legislated in British Columbia, the importance of ensuring that PIPA's mandatory breach notification rules align with PIPEDA and Alberta's PIPA needs to be emphasized. Canadian businesses are often challenged by patchworks of rules across the country and the costs of complying with different rules cannot be ignored. Individuals also have an interest in harmonized rules. Many breaches transcend borders, affecting Canadians in multiple jurisdictions. Regardless of where a breach originates, individuals are entitled to be notified under similar rules.

Turning to my specific recommendations, as is the case with Alberta PIPA and PIPEDA, PIPA should define what qualifies as a "breach". Alberta PIPA's mandatory breach notification requirements are triggered where there is an "incident involving the loss of or unauthorized access to or disclosure of the personal information".[11] PIPEDA refers to the "loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards".[12] These definitions offer sound guidance for PIPA.

Next, PIPA should not require organizations to give notice of all breaches. Again, breach notification rules help protect individuals against harm and incentivize organizations to protect personal information properly. Requiring organizations to notify in isolated trivial cases, where there is no reasonable prospect of harm to anyone, would achieve neither of these objectives and would impose unnecessary compliance costs on organizations. Setting too low a threshold for notice could also cause 'notification fatigue', i.e., the risk that, over time, individuals will become numb to breach notices and fail to take the steps they should when a serious breach actually does occur.

Neither Alberta PIPA nor PIPEDA require notification of all breaches. They both require notification only where there is a "real risk of significant harm" to an individual. The language differs slightly, but both statutes set out an objective test, i.e., it must be reasonable to believe that there is a real risk of significant harm to an individual. By focusing on "real risk" and "significant harm", both statutes set an appropriate threshold for triggering notification. This should be the test under PIPA. In addition, PIPEDA contains a non-exhaustive definition of

[11] Section 34.1.

[12] Section 2(1). I do *not* recommend using the concept of a "breach of security safeguards". Notification should not depend on their being a "security" breach. If someone's personal information has been compromised in one of the ways described above, it should qualify for notification if the harms test is met, whether or not there has been a breach of a "security safeguard". For example, if an organization's employee sets out to steal customers' personal information by walking out the door with paper copies, it is hard to see how a "security safeguard" could realistically prevent this.

"significant harm",[13] and a definition of the term "significant harm" could be considered for inclusion in the PIPA provisions.

The Alberta and federal laws differ on the issue of who should be notified. Alberta PIPA requires an organization to notify the Commissioner of a breach, and the Commissioner is empowered to require the organization to notify the affected individuals. PIPEDA requires an organization to notify affected individuals and the Commissioner, but without any authority for the Commissioner to order individual notification if that has not happened.

A combination of these rules is desirable. PIPA should require organizations to notify both affected individuals and my office of a breach. It should also authorize the Commissioner to require an organization to give notice to affected individuals if that has not happened, including where the Commissioner learns of the breach other than from the affected organization. PIPA should also enable the Commissioner to require an organization to give a general notice—e.g., in a newspaper or another kind of publication—where direct notice to each affected individual is impractical.

Both Alberta PIPA and PIPEDA have rules about when notice must be given and PIPA should similarly have timeliness requirements for notice, to ensure that notices are not stale-dated and thus possibly worthless as an instrument to protect individuals.[14]

In addition, PIPA should, as both PIPEDA and Alberta PIPA do, specify what information must be provided to the Commissioner and to individuals in a notice. My office's 2014 submission on the previous PIPA review listed the information elements that organizations should be required to include in notices to the Commissioner and to individuals, but the key is to ensure, as far as possible, that the PIPA requirements are in harmony with those in PIPEDA and Alberta PIPA. PIPA should also, like PIPEDA, require organizations to keep records of breaches they have experienced, with the contents of these records—which should be accessible to the Commissioner—being prescribed. This is supported by my colleague, the Privacy Commissioner of Canada.

To conclude, a significant number of the submissions you have received, from businesses and other organizations, support bringing PIPA in line with other Canadian privacy laws by introducing a duty to give notice of certain privacy breaches. Since the beginning of 2010 my office has received some 709 voluntary breach reports, so it is clear that the wider business community has long recognized the benefit of giving notice. A legal duty to do so would give them greater certainty about what they need to do and when. It also would give individuals

---

[13] Section 10.1(7) defines significant harm as *including* "bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property."

[14] Section 10.1(6) of PIPEDA, for example, requires the organization to give notice to affected individuals "as soon as feasible after the organization determines that the breach has occurred".

much greater comfort, knowing that they will be notified in a timely way that their personal information has been compromised, equipping them to take steps to protect themselves.

My office has urged a breach notification framework for years, starting with the first statutory review in 2008, and again in 2014, during the second review. Both the earlier Special Committees recommended that breach notification be included in PIPA and I urge you to do the same.

RECOMMENDATION 1

Amend PIPA to:

- Require organizations to notify affected individuals and the Commissioner of incidents involving the loss of, or unauthorized access to or disclosure of, personal information where it is reasonable to believe that there is a real risk of significant harm to an individual.
- Authorize the Commissioner to require an organization to notify affected individuals where the organization has not done so.
- Contain requirements relating to the timing of notice, the contents of notices, supporting information that must be provide to the Commissioner, and record-keeping duties for organization about the incidents they have experienced over time.

The amendments should be crafted to harmonize as far as possible with the similar provisions in Alberta's *Personal Information Protection Act* and the federal *Personal Information Protection and Electronic Documents Act*.

Protecting personal information transferred to service providers

Many organizations rely on contractors to perform various business functions that involve the personal information of organizations' customers or clients. Common examples of this include payroll processing services offered to businesses by specialist companies, and cloud-based software-as-a-service functions. The outsourcing of business functions undoubtedly can help make organizations more efficient by eliminating associated capital and operating costs.

Unlike other Canadian and global private sector privacy laws, however, PIPA does not expressly hold organizations responsible for their service providers. My office's view is that PIPA's

security requirements extend to information provided by an organization to a third party for processing. However, specific provisions in PIPA would be valuable in clarifying this matter and ensuring consistency with other regulatory frameworks.[15]

As for Canadian privacy laws, PIPEDA explicitly states as follows:

> An organization is responsible for personal information in its possession [control] or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.[16]

Similarly, Alberta PIPA provides that, "where an organization engages the services of a person, whether as an agent, by contract or otherwise, the organization is, with respect to those services, responsible for that person's compliance with this Act."[17]

Quebec Bill 64 will be even more explicit about this responsibility. It will require organizations that disclose personal information to a service provider to have a written services agreement with the service provider. Any agreement between an organization and a service provider must include the following:

- the measures the service provider must take to protect the personal information;
- provisions ensuring that the information is used only for performing the services;
- provisions ensuring that the service provider does not keep the information after the expiry of the contract;
- a requirement that the service provider must notify the outsourcing organization without delay of any violation or attempted violation by any person of any obligation concerning the confidentiality of the information communicated; and
- a power for the outsourcing organization to conduct any verification relating to confidentiality requirements.[18]

A similar approach to outsourcing is found in the GDPR, which contains detailed requirements for written outsourcing agreements between organizations and their service providers.[19]

The detailed approaches of Quebec Bill 64 and the GDPR need not be replicated in PIPA. PIPA should instead be amended to require organizations to use contractual clauses to ensure that personal information is protected in such situations. PIPA need not be as prescriptive as Quebec Bill 64 or the GDPR about the contents of these contracts. Organizations would have

---

[15] For example, section 4(2) of PIPA also states that an organization is "responsible for personal information under its control, including personal information that is not in the custody of the organization".
[16] Section 5(1) and clause 4.1.3 of Schedule 1 to PIPEDA.
[17] Section 5(2).
[18] These requirements are all set out in section 107 of Quebec Bill 64.
[19] GDPR, Article 28(4).

room to craft contracts that are best suited to each service arrangement but they would still be legally required to protect personal information that they transfer to their service providers.

My office urged this approach during the 2008 and 2014 reviews and several organizations that made submissions to you support it as well. Most important, both the previous Special Committees made this recommendation, as I urge you to do, noting that my recommendation would further harmonize PIPA with Alberta PIPA and PIPEDA.

RECOMMENDATION 2
Amend PIPA to state the following: • organizations are responsible for the personal information they transfer to a third party for processing or for providing services to or on behalf of the transferring organization; and • organizations must use contractual or other means to ensure compliance with PIPA, or to provide a comparable level of protection, for personal information they transfer to a third party for processing or for providing services to or on behalf of the transferring organization.

PRIVACY RIGHTS OF INDIVIDUALS

Modernizing consent requirements

PIPA respects the foundational importance of individual consent in private sector privacy laws. Its default position is that organizations cannot collect, use or disclose an individual's personal information without that individual's consent.[20] An organization that wants to collect someone's personal information must disclose the purposes for the collection, either before or at the time of collection. If the individual, armed with that information, consents to the collection, the organization can collect the information.[21] It can then use and disclose that information within the limits of the consent. This is one way in which PIPA implements its explicitly stated objective of enabling individuals to protect their personal information, while respecting the organizations' need for personal information.[22]

[20] Like all private sector privacy laws, however, PIPA provides exceptions to the requirement for consent to collection of personal information (and thus consent to use or disclosure of personal information).
[21] Section 8(1) of PIPA also recognizes, however, that some basic transactions are so straightforward that organizations ought not to be required to give formal notice or get formal consent, in writing or verbally. (PIPA contains other rules about collection of personal information. These include rules about how much personal information can be collected and the limitation that the collection purposes must be such that a reasonable person would consider them appropriate in the circumstances.)
[22] PIPA, section 2, states these legislative objectives.

PIPA's approach to consent to a large degree assumes that a bilateral transaction is involved, a transaction between one organization and a single individual. The organization tells the individual what it wants to do with the individual's personal information, the individual agrees, and the organization moves forward. This assumption may have been adequate when PIPA was drafted the better part of 20 years ago, but the modern information ecosystem threatens its relevance.

This is true for several reasons. One is the increasing dominance of technology services. As the globally active corporate giants expand their digital services footprint it will become more and more difficult for us to participate fully in society and in economic activity without using their services. The technology firms will tell you that they honour the notice and consent model reflected in PIPA. However, anyone wishing to use most of the large tech firms' services has no choice but to agree to their terms: the firms give notice of their intentions, but users have no choice in the matter.

As the small group of leading tech firms becomes ever-more dominant, individuals will not be able to find more congenial privacy terms elsewhere. This take-it-or-leave-it attitude on the part of many technology firms means that, while there is clearly still a need for notice-and-consent under PIPA, in the digital services realm individuals need enhanced protections beyond an updated approach to consent. This is the reason for my later recommendations about data analytics and profiling, data portability and the right to deletion of one's own personal information in certain circumstances.

It is nonetheless clear that, even in the context of the take-it-or-leave-it approach of many technology firms, PIPA's approach to notice and consent needs improvement, by requiring greater transparency about what organizations intend.

The privacy notices that many online businesses use are legalistic and detailed. They can be so lengthy that they take hours to read aloud, while managing to be imprecise about the purposes for which individuals' information will be used.

It is still all too common to see organizations use privacy notices that say something like, "We will use the information you give us or that we collect from other sources to improve the goods or services we or our partners may offer to you and you consent to this". This is so open-ended and obscure as to be meaningless. It leaves individuals in the dark about who will do what with their information. It obscures the very often complex flows of their data among various businesses. It is also not transparent about what technologies, such as AI, might be used to process an individual's information, and what might be done with a resulting personal profile. It is little wonder that we often click "I agree" without knowing what we are agreeing to—or having much, if any, ability to do anything about it.

This is not a new phenomenon and several private sector initiatives have been pursued over many years to encourage use of short, clear, and plain language, notices. These efforts are laudable, but the better approach is to legislatively bolster what is required.

One PIPEDA reform that the federal government has considered is to require organizations to give individuals specific, comprehensive and plain language information about the intended uses of their personal information and about any third parties with whom that information will be shared.[23] More concretely, the Quebec Bill 64 amendments will require that an individual's consent be "clear, free and informed". Consent must also "be given for specific purposes", and the request for consent must be stated "in clear and simple language and separately from any other information provided to the person concerned." Further, an organization will be obliged to, if an individual requests it, provide "assistance…to help [them] understand the scope of the consent requested."[24]

As noted earlier, PIPA currently requires an organization to disclose to an individual the purposes for which the individual's personal information is being collected. This can be done verbally or in writing. PIPA should be amended to address three aspects of its current approach to notice and consent.

The first change concerns notice requirements under PIPA. Section 10(1) permits organizations to give notice "verbally or in writing". However, the current evolving landscape of complex personal information flows, in situations involving powerful new digital technologies, makes it clear that verbal notice is no longer adequate. PIPA should explicitly require organizations to provide notice in writing to ensure that individuals understand what their personal information will be used for.

The second change involves the quality of the notice itself, which will ensure that the consent is meaningful. Consistent with PIPEDA and Quebec Bill 64, a new subsection 10(1.1) should be enacted that captures these concepts:

> The notice given under subsection (1) must clearly and plainly describe all of the purposes for which the personal information is being collected, used and disclosed, such that it is reasonable to expect that an individual would understand the nature, purpose and consequences of the collection, use or disclosure to which they are consenting.

The third change would amend PIPA to require organizations to set out the privacy consent language separate from other legal terms, and to assist an individual to understand what they are being asked to agree to if the individual asks.

---

[23] This and other possible PIPEDA amendments have been circulated by Innovation, Science and Economic Development Canada, a federal department: "Strengthening Privacy for the Digital Age". Accessed August 21, 2020.

[24] The amendments quoted in this paragraph are all found in section 102 of Quebec Bill 64.

This would not affect the ability of organizations—including small businesses—to rely on PIPA's existing deemed consent provisions. As noted earlier, section 8(1) of PIPA provides that an individual is "deemed to consent to the collection, use or disclosure of personal information by an organization for a purpose" if that purpose would be considered obvious to a reasonable person and the individual voluntarily provides the information.

For example, a dry-cleaning customer who is asked to provide their name and personal phone number for the dry-cleaning ticket surely consents to the dry cleaner collecting that information so as to be able to contact the customer if necessary. PIPA does not require the dry cleaner to give any notice of collection at all, either verbal or written. PIPA's deemed consent provision will capably continue to deal with these small business examples, i.e., situations where less sensitive personal information is collected for straightforward, ordinary-course purposes.[25]

Several of the submissions made by organizations to you discussed consent, with a range of perspectives among their submissions. Some of them have underscored that British Columbians legitimately expect that consent should be based on full disclosure and clearly explained terms.[26] I believe that my recommendation on this issue strikes the right balance between organizations' interests and individuals' privacy rights.

RECOMMENDATION 3

Amend PIPA to:

- Require organizations to give notice in writing to ensure that individuals understand what their personal information will be used for, unless consent is implied.
- Require organizations to provide comprehensive, specific, clear and plain notice of all purposes for which individuals' personal information will be collected, used and disclosed, such that it is reasonable to expect that an individual would understand the nature, purpose and consequences of the collection, use or disclosure to which they are consenting.
- Require organizations to provide notice separate from other legal terms, and to assist any individual to understand what they are being asked to agree to if the individual asks.

[25] In any case, in the dry-cleaning situation, the dry cleaner could easily post a collection notice at the point of service and draw customers' attention to it. This already a good practice and it is hardly burdensome to expect.
[26] As illustrated in, for example, the results of the public opinion survey conducted earlier this year by the BC Freedom of Information & Privacy Association, referred to in its joint submission with the BC Civil Liberties Association.

Aligning individuals' privacy rights with international legislative trends

As noted earlier, the GDPR, the California Act, and Quebec Bill 64 all represent significant shifts internationally to the legislative protection of our privacy. These and other recent privacy laws recognize that the change in information technologies and business practices affecting our privacy demand modern privacy protections for individuals.

The Special Committee has an opportunity through this review to recommend meaningful enhancements to the privacy rights of British Columbians. In addition to my other recommendations for PIPA's modernization, I urge you to adopt the following recommendations for enhancing everyone's privacy rights.

Automated decision-making notice and rights

Information technologies are evolving in ways, and at rates, that pose grave challenges for their appropriate regulations. Recent advances in data analytics and artificial intelligence offer great promise for improved services in both the public and private sectors. It is already clear, however, that they also pose risks for our privacy and other rights.

Privacy laws such as PIPA have traditionally assumed that transparency and individual consent offer sufficient core privacy protections. As outlined earlier, notice and consent are more and more under pressure in the context of modern technologies such as artificial intelligence and data analytics. Nor is there enough transparency on the part of the organizations or governments that are adopting these technologies.

Legislators are recognizing that more is needed. The GDPR contains robust protections for individuals in relation to automated processing of personal information to profile individuals.[27] With some exceptions, it gives individuals the right to object to profiling and prohibits an organization from making a decision about someone that is "based solely on automated processing, including profiling, which produces legal effects" concerning the information, "or similarly significantly affects" the individual.[28]

Closer to home, Quebec Bill 64 takes a less uncompromising yet welcome approach. When in force, the Quebec amendments will require organizations making decisions "based exclusively on an automated processing" of personal information to notify the affected individuals. Unlike the GDPR, Quebec Bill 64 will not give an affected individual the right to, effectively, veto the automated decision-making. It will, however, give the individual a right to be heard, i.e., a right to be told "the reasons and the principal factors and parameters that led to the decision".

---

[27] Article 4 of the GDPR defines "profiling" as the "automated processing of personal data" to "evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."

[28] GDPR, Article 22.

The individual will also have a right "to have the personal information used to render the decision corrected", which supports organizations' duty to use accurate and complete personal information. Last, Quebec Bill 64 will require organizations to give affected individuals an "opportunity to submit observations" to someone within the organization "who is in a position to review the decision".[29]

The GDPR enables individuals to effectively veto automated processing in some situations, but the Quebec amendments will not go that far. PIPA amendments like those in Quebec Bill 64 would complement organizations' existing duties around accuracy, completeness and correction of personal information and offer meaningful protections for individuals in automated decision-making processes. This approach, in contrast to the GDPR approach, would be consistent with PIPA's twin legislative objectives, of enabling people to protect their personal information while enabling organizations to use personal information for reasonable purposes.

RECOMMENDATION 4

Amend PIPA to require an organization using automated processing to:

- notify an individual that automated processing will be used to make a decision about them;
- on request, disclose the reasons and criteria used; and
- receive objections from individuals to the use of automated processing by someone within the organization that has the authority to review and change the decision.

Right to be forgotten (de-indexing)

Another area for possible reform in the context of international trends in privacy protection is the so-called right to be forgotten. As I have already noted several times, the expanding scope of digital services and the ever-increasing presence of digital technologies in our lives can have grave implications for control of our personal information.

This can include challenges raised by the online publication of our personal information without consent. Personal information in newspapers or other offline publications is not universally and permanently available. The historical privacy protection of practical obscurity is now more or less gone. Once a publication is posted online and is indexed in a search engine such as Google or Bing, it is universally and, effectively, permanently available around the world. This information might be inaccurate, incomplete, or outdated and thus not relevant or accurate, yet have the potential to permanently damage our reputations.

[29] These amendments will all be introduced by section 102 of Bill 64.

Concerns about these and other implications for individuals have led courts and legislators around the world to look for solutions that do not unreasonably impinge on other important principles and rights, notably freedom of expression.

The GDPR, for example, gives an individual the right to require an organization to erase the individual's personal information where, among other grounds, the personal information is no longer necessary for the purpose for which it was collected or the individual withdraws consent.[30] The organization can refuse an individual's request where the use or disclosure of the personal information is "necessary" for exercising its freedom of expression.[31]

Another form of the right to be forgotten is found in Quebec Bill 64. The amendments will permit an individual to require an organization to rectify information that is inaccurate, incomplete, or equivocal.[32] They will go further, however, by introducing a new right for individuals to require organizations to cease disseminating the individual's information, or "to de-index any hyperlink attached to [their]name that provides access to the information by a technological means"—or to "require that the hyperlink providing access to the information be re-indexed"—where several conditions are met. Those conditions, and the factors that must be considered in assessing the request, are complex and potentially onerous for organizations to apply.[33]

It should be noted that PIPA already offers some protection from use of outdated and therefore inaccurate personal information. PIPA requires organizations to destroy personal information, or render that information unidentifiable, "as soon as it is reasonable to assume that…the purpose for which that personal information was collected is no longer being served by" its retention (and retention is not necessary for legal or business purposes).[34]

In this context, I will limit my submission to asking you to recommend that the provincial government monitor policy and legislative developments in this area, globally and at home, to ensure that PIPA remains in harmony with similar laws.

---

[30] GDPR, Article 17.
[31] GDPR, Article 17(3)(a). Other refusal grounds include public health uses, archival or research uses, legal claims, and more.
[32] Quebec Bill 64, section 113.
[33] The conditions can be summarized as follows: whether the dissemination of the information causes the individual serious injury in relation to[their] right to the respect of [their] reputation or privacy; the injury is clearly greater than the interest of the public in knowing the information or the interest of any person in expressing himself freely; and whether ceasing the dissemination, or the re-indexation or de-indexation, exceeds what is necessary for preventing the perpetuation of the injury. The factors to be considered in assessing whether the conditions are met are as follows: whether the individual is a public figure or a minor; whether the information is up to date and accurate; the sensitivity of the information; the context in which the information is disseminated; the time elapsed between the dissemination of the information and the request; and, where the information concerns a criminal or penal procedure, the obtaining of a pardon or the application of a restriction on the accessibility of records of the courts of justice.
[34] PIPA, section 35(2).

RECOMMENDATION 5
The provincial government should continue to monitor developments in the area of the so-called right to be forgotten, to ensure that PIPA continues to protect individuals from the impact of use or disclosure of outdated, inaccurate or incomplete personal information (including through indexing by internet search engines).

Right to data portability

It is now routine for services across a broad spectrum of our lives to be entirely or largely electronically delivered. These involve compilation of large amounts of our personal information, ranging from service registration information to information about our service transactions over years. An underlying premise of modern privacy laws is that individuals are entitled to reasonable control of their own personal information. This includes the right to obtain access to one's own personal information.

Legislators have started to acknowledge that the right of individuals to control their own personal information should include a right, in the context of electronically delivered services, to obtain that information and, in effect, take it elsewhere. The GDPR right to data portability recognizes this by giving individuals the power to obtain their own personal information "in a structured, commonly used and machine-readable format", and to transfer that information to another organization without interference.[35]

This right enables individuals to use their own personal information as they wish. They may obtain their information from one service provider and transfer it to a competitor who is offering a better deal, or they may use their information for a different kind of service.

This enhancement to the principle of individual control of personal information may also have economic benefits because it can sharpen competition among businesses and may help prevent personal information monopolies from forming. From a more technical perspective, requiring organizations to provide personal information in a structured, commonly used, and machine-readable format promotes interoperability.

The trend toward data portability rights continues. Quebec Bill 64 will incorporate this right into that province's private sector privacy law.[36] The federal government's *Digital Charter* proposes

[35] GDPR, Article 20. This right only applies where the first organization was processing the individual's information by automated means: Article 20(1)(b). Article 20(1)(a) further restricts the portability right to situations where the first organization was processing the personal information based on, in essence, the individual's consent.

[36] Quebec Bill 64, section 112. The Quebec law will, among other things, provide that "computerized personal information collected from the applicant must, at [their] request, be communicated to him in a structured,

that individuals should have "clear and manageable access" to their own personal information, and "should be free to share or transfer it without undue burden."[37] Outside Canada, the California Act includes such a right,[38] and economies as diverse as India, Brazil, Thailand and Kenya have legislated data portability rights.

RECOMMENDATION 6
Amend PIPA to give individuals the right to obtain their own electronic personal information from an organization in a structured, commonly used, machine-readable format, at no expense to the individual. The organization should also be required to transfer, on request, personal information to an organization that the individual designates if it is technically feasible to do so without undue cost to the organization. This right should be subject to limits (e.g., whether the transfer is technically feasible, whether the request would interfere with a law enforcement matter or prejudice the legal rights of the organization).

COMMISSIONER'S OVERSIGHT POWERS

Administrative monetary penalties

British Columbians understand the evolving risks to their privacy flowing from technologies such as data analytics, artificial intelligence, facial recognition and more. They rightly expect that their privacy is backstopped by the same kinds of robust enforcement powers as exist in other areas, such as workplace health and safety and elections. They would be disappointed to learn this is far from the case under PIPA.

PIPA is, bluntly stated, largely toothless when it comes to enforcement of British Columbians' privacy rights. The most the Commissioner can do to sanction even a serious, wilful violation of their statutorily protected rights is, in effect, to order an organization to do what it should have done in the first place—fulfil its legal duty under the law. While it is an offence for an organization not to comply with a Commissioner's order, the decision to prosecute rests with the Criminal Justice Branch of the Ministry of Attorney General and the outcome of any prosecution is of course uncertain.

commonly used technological format. The information must also be communicated, at the applicant's request, to any person or body authorized by law to collect such information."

[37] Principle 4 of the *Digital Charter*. If pursued, this right would almost certainly be implemented through PIPEDA.

[38] Sections 1798.100, 1798.110, 1798.130 and 1798.145.

This is hardly reassuring to British Columbians who expect their privacy to be taken seriously, by being backed up with, where necessary, meaningful enforcement measures and sanctions. My office has always emphasised an educational, or remedial, approach to compliance and we will continue to work with individual organizations, business groups, civil society, and others to secure compliance by persuasion and education wherever possible.

This makes good sense, of course, but the reality is that there are some bad actors out there who will not honour their obligations under the law. This is detrimental for individuals whose privacy is at risk. It is also not fair to organizations who do comply with the law while bad actors may get away with not doing so.

Below I urge you to recommend that PIPA should enable the Commissioner to enforce an order through the courts. This is an important and much-needed tool, but it should not be the only enforcement tool. What is needed is a flexible and meaningful power for the Commissioner to, in appropriate cases, impose a monetary penalty on an organization. My office called for this power to be included in PIPA in 2008 and I am firmly convinced that this enforcement tool is an indispensable instrument for sanctioning the worst offences, while deterring them from occurring in the first place.

This enforcement tool is already commonplace across a range of regulatory fields in British Columbia. For example, the *Lobbyists Transparency Act* empowers me, as the Registrar of Lobbyists, to levy monetary penalties in appropriate cases. Other examples are the Chief Electoral Officer, who can levy monetary penalties under the *Election Act*, the BC Securities Commission, which can levy penalties under the *Securities Act*, and WorkSafeBC, which has that authority under the *Workers Compensation Act*.

In the privacy realm, Canada's privacy regulators in 2019 called for the power to impose monetary penalties under the privacy laws they each oversee. Ontario's Information and Privacy Commissioner already has that power under the Ontario *Personal Health Information Protection Act*. Quebec Bill 64 will give Quebec's privacy regulator that power. The federal government has indicated that it is considering giving the federal Commissioner that authority under PIPEDA. The Ontario government consultation paper on a provincial private sector privacy law for Ontario raises the possibility of monetary penalties in that law. The GDPR gives privacy authorities the power to impose significant monetary penalties and the UK's Information Commissioner has that authority under the *Data Protection Act, 2018*.

These powers are supported by several of the organizations that made submissions to you. These include the Canadian Bankers Association and Insurance Bureau of Canada, with civil society groups such as the Canadian Civil Liberties Association, BC Civil Liberties Association and BC Freedom of Information and Privacy Association also supporting monetary penalties. Amending PIPA to include monetary penalty powers would introduce an appropriate level of deterrence for bad actors. Monetary penalties would be reserved for the most serious violations of the law, for the worst offenders and the worst offences. The range of penalties

should address deterrence while being proportionate. In determining what would constitute an appropriate range, I recommend that the committee review those privacy jurisdictions that levy administrative monetary penalties to assess the appropriate fine levels in British Columbia. I encourage you to examine other jurisdictions to determine the appropriate levels for British Columbia.

The amendments should require the Commissioner, as does the *Lobbyists Transparency Act*, to follow due process before imposing a penalty, with a right for the organization to request a reconsideration. The courts would, of course, have oversight of the fairness and reasonableness of individual penalty processes and decisions.

The vast majority of British Columbia's organizations work in in good faith to comply with PIPA. However, PIPA's enforcement toolkit is lacking in the most serious cases, leaving British Columbians' privacy at risk. It is time for PIPA to come up to speed with other privacy laws, and with the other regulatory frameworks that already exist in British Columbia, by giving the Commissioner the power to impose monetary penalties.

RECOMMENDATION 7
Amend PIPA to enable the Commissioner to impose a monetary penalty on an organization for non-compliance with PIPA. The amendments should include due process and reconsideration requirements.

Responsive, flexible oversight through compliance agreements

As I have already underscored, administrative monetary penalties can be useful enforcement tools in the most serious cases. For less serious concerns, it may be sufficient to issue a formal compliance order to an organization, but this can only be done after a formal process is followed. There are cases, however, where non-compliant organizations are keen to comply when we bring the non-compliance to their attention. In such cases, a formal investigation and compliance order may be an unnecessary use of resources, with a compliance agreement offering a flexible and responsive solution.

Parliament has recognized the need for this flexible tool and PIPEDA now enables the federal Commissioner to enter into compliance agreements with non-compliant organizations. When this is done, formal enforcement activities cease.[39] Compliance agreements under PIPEDA contain any terms that the Commissioner considers necessary to ensure compliance with this Part."[40] If the Commissioner considers that the organization is not complying with the agreement, the Commissioner can apply to the court for an enforcement order or other

[39] As an exception, a compliance agreement does not stop a possible prosecution for an offence.
[40] PIPEDA, sections 17.1(1) and (2).

remedy.

Compliance agreements are increasingly common regulatory tools. In British Columbia, the *Workers Compensation Act* now authorizes WorkSafeBC to enter into compliance agreements, providing both regulatory certainty and flexibility for all concerned.[41] A similar power in PIPA would give my office a useful alternative from more formal enforcement measures, including monetary penalties, and should form part of the enforcement toolkit.

RECOMMENDATION 8
Amend PIPA to enable the Commissioner to enter into a compliance agreement with an organization on such terms as the Commissioner considers appropriate, with enforcement by the court in cases of non-compliance.

Improving regulatory information sharing and cooperation

We have seen how dramatically things have changed for our privacy since PIPA was enacted almost 20 years ago. The myriad of ways in which our personal information is harvested and used now routinely extends beyond British Columbia's borders, making the challenges to our privacy a truly cross-border phenomenon. Not surprisingly, privacy enforcement actions are increasingly trans-border in nature. My office, for example, recently completed an investigation with my Ontario counterpart into a privacy breach at LifeLabs.

PIPA supports our domestic enforcement cooperation by enabling the Commissioner to exchange information with other Canadian privacy regulators.[42] It also authorizes the Commissioner to enter into agreements with them for the purpose of coordinating their activities and providing mechanisms for complaints.[43] These are useful powers and my office has used them successfully in investigations such as those just mentioned. PIPA's domestic information sharing, and cooperation powers should, however, be reviewed to ensure that they continue to align satisfactorily with the comparable but more fulsome Alberta PIPA and PIPEDA provisions.

In recent years I have encountered situations where privacy regulator colleagues outside Canada wish to cooperate with us in ways that would require enhanced information sharing and cooperation powers. Our ability to share information with privacy regulators outside Canada should be clarified, to better support our working cooperatively with regulators elsewhere, such as the Federal Trade Commission and the UK Information Commissioner's Office. For this reason, to eliminate doubt, PIPA should be amended to explicitly enable the

[41] *Workers Compensation Act*, section 83.
[42] PIPA, section 36(1)(k).
[43] PIPA, section 36(1)(l).

Commissioner to enter into information-sharing and cooperation agreements with foreign privacy regulators.

RECOMMENDATION 9
Amend PIPA to explicitly enable the Commissioner to enter into information-sharing and cooperation agreements with foreign privacy regulators.

Enhancing and clarifying Commissioner oversight powers

My June submission to you noted that PIPA does not explicitly permit the Commissioner to make an order in the absence of a complaint. As explained below, this is a weakness in enforcement powers and this gap should be filled.

As noted above, the complexities involved in today's digital world mean that individuals may not be aware of how their personal information is being collected, used, and disclosed. That complexity makes it very difficult for any one individual to identify contraventions of PIPA and bring them to my office's attention through a complaint. Individuals are too often just not able to get at the information necessary to do this. PIPA does authorize the Commissioner to initiate an investigation or audit without a complaint, but it is so restrictive that it does not fill the gap. At present, the Commissioner can initiate an audit or investigation where the Commissioner "is satisfied there are reasonable grounds to believe that an organization is not complying with" PIPA. This threshold is unnecessary, and it contrasts starkly with FIPPA, which contains no "reasonable grounds" requirement for a Commissioner-initiated audit or investigation.

Audits of organizations' privacy practices can be beneficial for the organization just as much as the public interest. They can be quite informal, and my office approaches them as educational, or remedial, in nature. They are also cost-effective. This has been shown time and again under FIPPA. To require the Commissioner to have "reasonable grounds" to believe that an organization is "not complying" with PIPA imposes an unnecessary threshold for selecting this compliance tool. It is also an inappropriate standard for starting a formal investigation under a non-criminal regulatory framework such as PIPA. Further, given the complexity of data flows, and the lack of transparency that too often surrounds them, if it is not possible for individuals to become aware of concerns, so they do not complain, it is hard to see how the Commissioner could become aware of information that reasonably suggests an organization is not complying with the law.

The "reasonable grounds" threshold, in other words, is completely archaic in the modern context and poses a threat to responsive, proactive oversight of organizations' compliance with the law. This aspect of PIPA should be amended so that it aligns with FIPPA, by removing the requirement for "reasonable grounds" before the Commissioner can start an investigation without a complaint.

Another issue is PIPA's lack of clarity about whether the Commissioner can issue a compliance order after an investigation that the Commissioner has initiated without a complaint. While I consider this power exists, some have called it into question, arguing that the Commissioner's order-making power can only be used where the Commissioner has held an inquiry into a complaint by an individual, not a Commissioner-initiated investigation.[44] This should be made clearer, as is the case under FIPPA. The last Special Committee agreed and recommended that PIPA should enable the Commissioner to make an order after a Commissioner-initiated investigation.

A third concern is that, at present, PIPA does not clearly enable the Commissioner to enforce an order against an organization by filing it in court, which makes it an order of the court. This is another difference between FIPPA and PIPA, since FIPPA expressly permits the Commissioner to file an order in court. There is no valid reason for this situation to continue.

These three examples of PIPA's inadequacy in the area of enforcement speak clearly to the need for broader reform of PIPA's enforcement provisions. Parts 10 and 11 of PIPA should be completely revamped, to align them with the Commissioner's enforcement powers under FIPPA. My office called for this reform in 2008 because of the needless complexity in Parts 10 and 11 of PIPA. As noted in that submission, these aspects of PIPA suffer greatly from inconsistent terminology, and difficult to understand, even cryptic, language. The first Special Committee agreed, noting that reform of Parts 10 and 11 "would make the legislation more accessible and understandable to the general public", and that aligning PIPA and FIPPA in this respect would "promote clarity and further harmonization". This is true. It is also true that this alignment would enhance our processes' efficiency, supporting the timeliness and quality of our work.

The minimum necessary amendments, however, are removing the "reasonable grounds" threshold for a Commissioner-initiated investigation, clarifying the Commissioner's order-making power, and explicitly enabling the Commissioner to file orders in court.

To remedy the inconsistency between FIPPA and PIPA in relation to order-making powers and improve the Commissioner's enforcement tools, I am making the same recommendation made by the previous Commissioner in her 2014 submission and by the previous Special Committee in its report to government.

[44] PIPA, section 52(3).

RECOMMENDATION 10
Amend PIPA by replacing the Commissioner's enforcement powers in Parts 10 and 11 with powers substantially the same as the powers in Parts 4 and 5 of the *Freedom of Information and Protection of Privacy Act*. At a minimum, amend PIPA to: • remove the "reasonable grounds" threshold for Commissioner-initiated audits or investigations; • to clarify the Commissioner's order-making power in Commissioner-initiated investigations; and • to enable the Commissioner to file orders in court.

OTHER NECESSARY AMENDMENTS

Clarifying PIPA's relationship to PIPEDA

My office has historically enjoyed excellent working relations with colleagues across the country. This continues to be the case, as our recent joint investigations with the federal and the Ontario Commissioners demonstrate. Overlap between provincial and federal laws and regulatory responsibilities is a well-known feature of Canadian federalism and it can be managed well. Our work with our federal and provincial colleagues reflects the fact that, although federal and provincial agencies may both have roles in regulating conduct, we are able to work well together. I am confident this long tradition will continue.

Nonetheless, I am concerned that PIPA contains clauses that, in theory, could unnecessarily cloud the situation.

Specifically, section 3(2)(c) of PIPA provides that PIPA does not apply to "the collection, use or disclosure of personal information, if the federal Act [PIPEDA] applies to the collection, use or disclosure of the personal information." The result of this is that, even if PIPA would otherwise properly apply to a matter where PIPEDA also applies, this clause means PIPA abandons the field and leaves the matter exclusively to the federal Commissioner to handle. It is not hard to think of cases where the real connection of a matter is with British Columbia because it relates to an otherwise exclusively provincially-regulated, British Columbia-based organization, - yet PIPEDA may apply because of an even minor cross-border element.

There is no good public policy reason for British Columbia law not to apply in addition to federal law where both can properly apply. Surely it is appropriate for British Columbia law—and a British Columbia regulator—to have the primary role in regulating British Columbia organizations, even where there is possibly a minor inter-provincial aspect to a situation.

Another significant potential issue also arises. Down the road, there may be cases where section 3(2)(c) ousts PIPA's application, but the federal Commissioner is either unable or unwilling to address the matter. The federal Commissioner's enforcement priorities may result in a serious concern that largely involves a British Columbian organization and British Columbians' privacy remaining unaddressed. Fiscal constraints may mean the federal Commissioner's enforcement resources are not deployed in such a case. This could leave British Columbians without a remedy for a possibly serious privacy violation, with no recourse to my office if the organization in question challenges our jurisdiction because of section 3(2)(c).

In contrast, Alberta PIPA does not contain such an unnecessary scope limitation. It has, since day one, taken the right approach, enabling cooperative Canadian regulation while not including a self-defeating provision like section 3(2)(c). This weakness in our law should be remedied by the repeal of section 3(2)(c).

RECOMMENDATION 11
Amend PIPA to harmonize with Alberta's *Personal Information Protection Act*, by repealing section 3(2)(c), which unnecessarily restricts PIPA's ability to protect British Columbians' privacy where both PIPA and PIPEDA apply.

RECOMMENDATIONS BY STAKEHOLDERS

Legal privilege and individuals' access to their own personal information

The Canadian Bar Association (BC Branch) and the Law Society of British Columbia have asked you to recommend amendments that would significantly change how claims of solicitor client privilege are decided under PIPA. The Law Society has asked you to ensure that such claims are decided by the courts, not the Commissioner, and the CBA's submission also mentions this.[45]

Both the previous Special Committees rejected similar requests from legal profession groups, and I ask you to do so now.

I will start by noting that one of the internationally recognized privacy rights reflected in PIPA is the fundamental right of individuals to request access to their own personal information in the hands of organizations. If an individual requests it, an organization must provide the individual's personal information under the control of the organization, information about the ways in

[45] However, the CBA's formal recommendations do not appear to include this request. The CBA does seek an amendment to section 38(5) of PIPA, to remove the Commissioner's ability to compel and view records that an organization claims are protected by solicitor client privilege. This is addressed below.

which the personal information has been and is being used by the organization, and the names of those individuals or organizations to whom that personal information has been disclosed.[46]

The right of access to one's own personal information, and to information about what an organization is doing with that information, is vitally important because it enables individuals to determine whether that information is accurate or complete (and if it is not, to request its correction). This right also empowers individuals to determine whether an organization has inappropriately collected too much information about them, has used information that it collected properly in an improper way, has disclosed personal information inappropriately, or has retained personal information for too long. The importance of the right of access to one's own personal information is therefore difficult to overstate.

An individual's right of access is not absolute, of course, and PIPA authorizes organizations to refuse to disclose an individual's personal information, and the other information described above, where the information is protected by solicitor client privilege.[47] This is entirely appropriate, of course, because an organization's legitimate interests may be harmed if privileged information is disclosed to someone, notably where the individual who made the request is adverse in interest to the organization.

My office on occasion is called to handle cases in which an individual has requested access to their own personal information and the organization has refused disclosure because of solicitor client privilege. As with all disputes, my office usually resolves these matters through mediation, not formal adjudication. Regardless of whether we are engaged in mediation or formal adjudication, it is our policy under PIPA, and under FIPPA, to resolve privilege claims without asking to see the allegedly privileged information unless it is absolutely necessary to do so. This is the same standard that the courts apply.

Where privilege is asserted, it is always open to an organization to disclose disputed records to my office (my office obviously never shares these records with the individual). PIPA does empower the Commissioner, however, to require an organization to provide an allegedly privileged record to the Commissioner for review, "[d]espite any other enactment or any privilege afforded by the law of evidence".[48] PIPA protects the privilege, however, by saying that, "if information to which solicitor client privilege applies is disclosed" to the Commissioner, "the solicitor client privilege is not affected".[49]

If mediation fails, the privilege issue can be decided through adjudication under PIPA. The Commissioner must decide, based on the evidence put forward by the organization—which has the burden of making out its privilege claim—whether a record is privileged. If either the organization or the individual does not agree with the Commissioner's decision, an application

[46] PIPA, section 23(1).
[47] PIPA, section 23(3)(a).
[48] PIPA, section 38(5).
[49] PIPA, section 38(3).

for judicial review may be made to the Supreme Court of British Columbia. The Court provides robust oversight of privilege decisions by applying the strict judicial review standard known as correctness. That standard means the Court owes no deference to the Commissioner's decision. The Court can substitute its own decision on the merits, by deciding the privilege question afresh, on the same evidence the Commissioner had. This is an appropriately robust protection for solicitor client privilege.

Another protection for privileged material is that my office *never* discloses privileged material to an applicant, or anyone else, during our complaint, audit or investigations processes. PIPA explicitly states that the Commissioner "must not" disclose information that an organization could or must withhold in response to an individual's access request and must take every reasonable precaution to avoid disclosing privileged information.[50]

Similarly, if an organization's privilege claim proceeds to adjudication, my office *never* discloses material that has been held, after a hearing, not to be privileged. PIPA says, rather, that the Commissioner may "require the organization…to give the individual access to all or part of [their] personal information".[51] This underscores the fact that it is always—always—the organization that discloses the information, never my office. If an organization thinks my office's privilege decision is wrong, or that its privilege is at risk, it can apply to the court for relief. If an organization does that, our order is automatically "stayed from the date the application is brought until a court orders otherwise".[52] If the courts overturn our decision to the contrary, the matter ends: the organization is not required to disclose anything.

Legal privilege is of fundamental importance to the Canadian legal system and the rights of Canadians. My office therefore takes special care in dealing with solicitor client privilege matters, as has been the case throughout the nearly 30 years of this office's existence. Our policies and processes are impartial, fair, rigorous, and efficient, offering individuals and organizations alike efficient access to justice under the watchful eye of the courts.

Turning to the Law Society and CBA submissions, the Law Society appears to suggest that a 2016 Supreme Court of Canada decision calls into question the previous Special Committees' view that PIPA authorizes the Commissioner to decide the privilege issue.[53] Respectfully, *University of Calgary* says *only* that the Alberta PIPA provision dealing with production of records is not expressed in sufficiently clear terms to capture allegedly privileged records.

The Law Society nonetheless says that, where "a principle of fundamental justice is at issue, the Courts should be the adjudicative authority", but this is a preference, not constitutional or legal destiny.[54] The Supreme Court of Canada did not say this in *University of Calgary* or in other

[50] PIPA, section 41(3).
[51] PIPA, section 52(1)(a)(i).
[52] PIPA, section 53(2).
[53] *Alberta (Information and Privacy Commissioner) v. University of Calgary*, 2016 SCC 53 [*University of Calgary*].
[54] Law Society submission, page 3.

cases the Law Society cites. By contrast, through PIPA the Legislature has explicitly tasked the Commissioner with the authority and duty to adjudicate the issue.
The Law Society nonetheless urges the Special Committee to recommend a process that would have the courts decide privilege claims. Doing so would raise a barrier to access to justice for individuals who have been denied access to their own personal information but cannot afford the considerable cost of challenging that claim in court. By contrast, the Law Society has not cited examples of harm to organizations (or public bodies) despite the nearly 30 years of timely and efficient adjudication of such questions by this office, always under the strict oversight of the courts.[55]

The CBA's submission to you makes some of the same points as the Law Society. These need not be discussed here. Nor is it necessary to discuss the Law Society's brief further. Rather, if the Special Committee wishes more detailed reasons for not recommending any changes to PIPA, it might wish to refer to the submission made by David Loukidelis.[56]

I am making the same recommendation made to the committee in 2008, and that the Special Committee recommended in its reports to government following the 2008 and 2014 consultations.

RECOMMENDATION 12
PIPA should not be amended to oust the Commissioner's role in deciding, under court oversight, if an organization's claim of solicitor client privilege has been established. Nor should the Commissioner's ability to view allegedly privileged records where absolutely necessary be removed.

CONCLUSION

Most laws lag behind developments in socio-economic conditions, business practices, technology, and public expectations. PIPA was enacted almost 20 years ago under conditions very, very different from those we live under today. Rapidly evolving digital technologies,

[55] The Law Society suggests that *University of Calgary* illustrates the risks to privilege, apparently because the outcome of that case was to overturn the decision of the Alberta Commissioner's office. This is hardly persuasive. For one thing, it is only a single case, one in which the courts ultimately disagreed with the decision of the Commissioner's office. This does not really advance the Law Society's position that only the courts can decide these issues. Further, that case amply illustrates how the courts play an important oversight role where judicial intervention is warranted on the merits, case by case.
[56] His submission is posted here: https://www.leg.bc.ca/content/CommitteeDocuments/41st-parliament/5th-session/pipa/submissions/1042-12558_Loukidelis-David_Submission.pdf. Accessed August 27, 2020.

business models and public attitudes toward privacy present very different challenges for privacy and ensuring a competitive environment for digital businesses.

As this submission demonstrates, PIPA is at serious risk of failing to meet these modern challenges. This submission therefore focuses on key legislative changes that are necessary if PIPA is to continue to strike the right balance between protecting privacy while helping to support British Columbia's economic development.

Your work is of vital importance in achieving that balance in a modernized PIPA. All British Columbians look forward to your report and to government's rapid, positive, response to your recommendations.

SUMMARY OF RECOMMENDATIONS

Recommendation 1: Mandatory breach notification
Amend PIPA to:

- Require organizations to notify affected individuals and the Commissioner of incidents involving the loss of, or unauthorized access to or disclosure of, personal information where it is reasonable to believe that there is a real risk of significant harm to an individual.
- Authorize the Commissioner to require an organization to notify affected individuals where the organization has not done so.
- Contain requirements relating to the timing of notice, the contents of notices, supporting information that must be provide to the Commissioner, and record-keeping duties for organization about the incidents they have experienced over time.

The amendments should be crafted to harmonize as far as possible with the similar provisions in Alberta's *Personal Information Protection Act* and the federal *Personal Information Protection and Electronic Documents Act*.

Recommendation 2: Protecting personal information transfer to service providers
Amend PIPA to state the following:

- organizations are responsible for the personal information they transfer to a third party for processing or for providing services to or on behalf of the transferring organization; and
- organizations must use contractual or other means to ensure compliance with PIPA, or to provide a comparable level of protection, for personal information they transfer to a third party for processing or for providing services to or on behalf of the transferring organization.

Recommendation 3: Modernizing consent requirements
Amend PIPA to:

- Require organizations to give notice in writing to ensure that individuals understand what their personal information will be used for, unless consent is implied.
- Require organizations to provide comprehensive, specific, clear and plain notice of all purposes for which individuals' personal information will be collected, used and disclosed, such that it is reasonable to expect that an individual would understand the nature, purpose and consequences of the collection, use or disclosure to which they are consenting.
- Require organizations to provide notice separate from other legal terms, and to assist any individual to understand what they are being asked to agree to if the individual asks.

Recommendation 4: Automated decision-making notice and rights
Amend PIPA to require an organization using automated processing to:

- notify an individual that automated processing will be used to make a decision about them;
- on request, disclose the reasons and criteria used; and
- receive objections from individuals to the use of automated processing by someone within the organization that has the authority to review and change the decision.

Recommendation 5: Right to be forgotten (de-indexing)
The provincial government should continue to monitor developments in the area of the so-called right to be forgotten, to ensure that PIPA continues to protect individuals from the impact of use or disclosure of outdated, inaccurate or incomplete personal information (including through indexing by internet search engines).

Recommendation 6: Right to data portability
Amend PIPA to give individuals the right to obtain their own electronic personal information from an organization in a structured, commonly used, machine-readable format, at no expense to the individual. The organization should also be required to transfer, on request, personal information to an organization that the individual designates if it is technically feasible to do so without undue cost to the organization. This right should be subject to limits (e.g., whether the transfer is technically feasible, whether the request would interfere with a law enforcement matter or prejudice the legal rights of the organization).

Recommendation 7: Administrative monetary penalties
Amend PIPA to enable the Commissioner to impose a monetary penalty on an organization for non-compliance with PIPA. The amendments should include due process and reconsideration requirements.

Recommendation 8: Compliance agreements
Amend PIPA to enable the Commissioner to enter into a compliance agreement with an organization on such terms as the Commissioner considers appropriate, with enforcement by the court in cases of non-compliance.

Recommendation 9: Improving regulatory information sharing and cooperation
Amend PIPA to explicitly enable the Commissioner to enter into information-sharing and cooperation agreements with foreign privacy regulators.

Recommendation 10: Enhancing and clarifying Commissioner oversight powers
Amend PIPA by replacing the Commissioner's enforcement powers in Parts 10 and 11 with powers substantially the same as the powers in Parts 4 and 5 of the *Freedom of Information and Protection of Privacy Act*.

At a minimum, amend PIPA to:

- remove the "reasonable grounds" threshold for Commissioner-initiated audits or investigations;
- to clarify the Commissioner's order-making power in Commissioner-initiated investigations; and
- to enable the Commissioner to file orders in court.

Recommendation 11: Clarifying PIPA's relationship to PIPEDA
Amend PIPA to harmonize with Alberta's *Personal Information Protection Act*, by repealing section 3(2)(c), which unnecessarily restricts PIPA's ability to protect British Columbians' privacy where both PIPA and PIPEDA apply.

Recommendation 12: Legal privilege
PIPA should not be amended to oust the Commissioner's role in deciding, under court oversight, if an organization's claim of solicitor client privilege has been established. Nor should the Commissioner's ability to view allegedly privileged records where absolutely necessary be removed.