STATUTORY REVIEW OF THE PERSONAL INFORMATION PROTECTION ACT

General briefing for the Special Committee to Review the Personal Information Protection Act

June 2020
Michael McEvoy
Information and Privacy Commissioner
for British Columbia

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

TABLE OF CONTENTS

PREFACE 2
INTRODUCTION 3
The Importance of Privacy 3
Privacy Protection in the Digital Age 3
LEGISLATION 4
The Personal Information Protection Act 4
Legislation Across Other Jurisdictions 5
RECENT WORK OF THE OIPC 6
Guidance and Outreach 6
Investigations 6
Complaints 8
Privacy Breach Investigations 8
Audit and Compliance Program 8
Recent Orders and Court Decisions 8
Inter-jurisdictional Collaboration 9
THE NEED FOR REFORM 9
Previous Statutory Review (2014) 9
Keeping Pace with National and International Trends 10
Commissioner's Recommendations 10
CONCLUSION 12
APPENDIX 13

PREFACE

The time to reform BC's private sector privacy law is now. BC needs to clarify, strengthen, and enhance privacy protection to meet citizens' expectations of personal information privacy in a new all-encompassing digital environment.

The digital world is already expanding at a rapid pace - its trajectory has now exploded with the advent of COVID-19. The pandemic has altered the way we work, communicate, shop, educate and more. This electronic revolution, transpiring right before our very eyes, requires privacy rules fit for purpose.

The truth is that BC has fallen behind the rest of the world when it comes to both protecting the privacy of our citizens and ensuring the province remains competitive in a world where digital commerce is on the rise. All of this means the outcome of the Special Committee's work will potentially have far reaching consequences for BC's place in this rapidly changing world.

I would submit that the Committee's work should not end with the issuance of its report to government. It will be critically important, charged with the knowledge gained from its investigations, that the Committee continue to urge government's decision-makers of the need to move forward.

My office looks forward to supporting the Committee's work and assisting in realizing the recommendations that result from its work.

June 2, 2020

ORIGINAL SIGNED BY

Michael McEvoy
Information and Privacy Commissioner
for British Columbia

INTRODUCTION

The Importance of Privacy

Privacy tends to be equated with keeping secrets. In some cases, that's true. But more fundamentally privacy is about the right and ability of an individual to exact control over that which is personal; their body, their physical space, or the information about them. The *Personal Information Protection Act* (PIPA) is focused on the last of these and it imposes limits on what personal information organizations can collect, use, or disclose about us. Its provisions are underpinned by the societal norms of a democratic society and its quasi-constitutional standing recognized by our highest court.

In the 2013 case of *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401* the Supreme Court of Canada stated:

> The ability of individuals to control their personal information is intimately connected to their individual autonomy, dignity and privacy. These are fundamental values that lie at the heart of a democracy. As this court has previously recognized, legislation which aims to protect control over personal information should be characterized as "quasi-constitutional" because of the fundamental role it plays in a free and democratic society.

Privacy protection is critical to the functioning of Canadian society. We expect our personal information to be protected in our day-to-day interactions with financial institutions, lawyers, health care professionals, and businesses. Individuals in a democratic society rightfully expect others to respect their privacy.

Privacy Protection in the Digital Age

Privacy protection is especially relevant and challenging in the digital age. Every minute of every day massive amounts of data elements are generated, making privacy protection more complex. Online commerce alone is growing exponentially.

Evolving technologies enable more and more data collection, data sharing, and sophisticated data analytics. Electronic databases make it easy and inexpensive to collect, store, and disclose personal information, with the capacity to indefinitely store endless amounts of data and readily disclose personal information to users, third parties, and even data brokers.

New technologies have also created an increasingly sophisticated world of data analytics that allow data to be mashed and manipulated through techniques such as data-mining and data-matching. Facial recognition technology can be applied to databases that store images.

Electronic surveillance is another technology with heightened privacy risks. The COVID-19 pandemic raised the public's awareness about privacy considerations around contact tracing

and temperature checking, among other surveillance mechanisms. These surveillance mechanisms should only be used in a privacy protective manner.

Social media serves as an example of a global privacy challenge. There is intense and lucrative demand for the very large "honeypots" of data collected by social media giants such as Facebook. Third parties wish to use that unique data for commercial, political, research and other inventive purposes. A groundbreaking and high-profile investigation in 2018 by the UK Commissioner with respect to the use of Facebook data by Cambridge Analytica and AggregateIQ alerted both the public and regulators of how data was being disclosed and misused for political purposes and the need for closer scrutiny and transparency. Our office and the Office of the Privacy Commissioner of Canada recently investigated Facebook and Victoria based company AggregateIQ. The US Federal Trade Commission and the Canadian Competition Bureau have also levied substantial fines against Facebook.

This egregious misuse of data also illustrates the pervasive lack of openness and transparency in certain sectors as to what data elements are being collected, how the data is used, and to whom it is disclosed and for what purpose. Privacy policies are often opaque and inaccessible. It is virtually impossible for the average person to assess whether proper security measures are in place to prevent hacking, ransomware attacks, or other cyber threats.

The massive flow of data across international boundaries also means that improperly protected personal information in one jurisdiction could result in a breach with worldwide ramifications. Investigations and enforcement of data management of these matters often require inter-jurisdictional collaboration.

Our province needs to do its part in this interrelated environment by upping standards to meet global benchmarks.

LEGISLATION

The Personal Information Protection Act

The *Personal Information Protection Act* (PIPA) is British Columbia's private sector privacy law. It was passed by the Legislature in 2003 and came into force a year later.

PIPA applies to more than a million organizations, including businesses, financial institutions, professional practices, non-profits, professional regulatory bodies, strata councils, trade unions, and political parties. It governs how those organizations handle personal information. Personal information is defined as information about an identifiable individual.

As stated in s. 2 of PIPA:

> The purpose of this Act is to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of individuals to protect their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

Individuals have a right to request their own information that organizations hold about them, as well as how it has been used. If an individual sees an error or omission, they can request that the organization correct it.

PIPA is consent based. This means that in most circumstances an organization must acquire the consent of the individual the information is about in order to collect, use, or disclose personal information for appropriate purposes. Consent is implied if an individual voluntarily provides personal information for an obvious purpose.

Legislation Across Other Jurisdictions

PIPA is one of five private sector privacy laws in Canada and was enacted in 2004. It followed the passage of a federal privacy bill (PIPEDA) in 2001 which did not apply in provinces that had "substantially similar" legislation. [1]

Both British Columbia and Alberta adopted almost identical provincial laws that were then deemed substantially similar. Quebec has a private sector privacy law that predates PIPEDA and has also been deemed substantially similar. Manitoba recently passed a private sector privacy law that is not yet in force.

All privacy laws in Canada are principles-based and reflect fair information practices. Fair information practices originated in European data protection laws and 1980 guidelines developed by the Organization for Economic Cooperation and Development. A 1995 European directive prohibited the electronic export of personal data to any country that does not have an adequate level of legal privacy protections. PIPEDA was deemed adequate when it was passed.

More recently, adequacy status is measured against the new European General Data Protection Regulation (GDPR). It was brought into force in 2018 and sets out a much higher level of privacy protection than what existed previously. It has gained recognition as the gold standard globally and has become the model for a number of national laws outside the European Union.

[1] It should be noted, however, that the *Personal Information and Electronic Documents Act* would continue to apply to all federally-regulated entities including, banks, railways, and telecommunication companies operating within a province.

Privacy laws underpin other important areas of law: commerce, international trade, and consumer protection. Strong privacy laws preserve the chain of assurance that facilitates international data flows. **The need for PIPA to remain substantially similar to PIPEDA and have adequacy status in relation to the GDPR cannot be overstated.**

RECENT WORK OF THE OIPC

The Commissioner is responsible for administering PIPA to ensure that its purposes are achieved. Section 36 of the Act sets out a non-exhaustive list of actions the Commissioner may take to do so. These include initiating investigations and audits, informing the public about the Act, commenting on the privacy implications of proposed initiatives of organizations, and investigating and mediating complaints. All these tools are aimed at ensuring compliance with PIPA, which at times can pose a challenge.

Privacy management programs are critical for building consumer trust and confidence in an organization's personal information management practices. British Columbians are sometimes surprised to learn that the Commissioner can investigate, but cannot penalize, bad actors who violate privacy laws.

That said, the Office does its best within its existing resources to protect British Columbians and require organizations to properly protect the personal information they possess. Below are highlights of recent work of the Office of the Information and Privacy Commissioner (OIPC).

Guidance and Outreach

The OIPC has an extensive and user-friendly website where accessible information and guidance is readily available to the public, to organizations, and to public bodies. The website is carefully monitored and kept up to date on a regular basis.

When new materials are posted, we may issue a media release and/or advise stakeholders directly that we have prepared guidance or other materials that are specifically relevant to them. See for example recent work focused on restaurants and bars collecting personal information for the purposes of contact tracing of COVID-19. These and other highlights of OIPC guidance and outreach activities in relation to PIPA compliance since the last statutory review are set out in Appendix A.

Investigations

AggregateIQ Data Services Ltd. (November 2019)

This joint investigation with the Privacy Commissioner of Canada concerned micro targeting and analytics in political campaign advertising based on repurposed and sensitive information

obtained from third parties. The information included psychographic profiles derived from Facebook data.

The report found that AggregateIQ (a BC-based company providing data-related services for UK, US, and Canadian political campaigns) failed to meet the consent requirements of PIPA and the Federal *Personal Information and Electronic Documents Act* (PIPEDA) for the collection, use, and disclosure of personal information. The company also failed to take reasonable security measures to ensure that personal information under its control was secure from unauthorized access or disclosure. The Commissioners made a series of recommendations that AggregateIQ agreed to implement.

Report of Findings: Joint investigation of Facebook Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia (April 2019)

This joint investigation with the Privacy Commissioner of Canada concerned the use of Facebook data for targeted political messaging. Facebook disclosed personal information of millions of its users to a third-party application (known as thisisyourdigitallife) that was subsequently used by third parties for targeted political messaging. There were three general areas of concern in terms of compliance with PIPA and PIPEDA:

- consent of users whose information was disclosed by Facebook to apps;
- safeguards against unauthorized access, use, or disclosure by apps; and
- accountability for the information under Facebook's control.

The Commissioners found that Facebook failed to obtain valid and meaningful consent of installing users and their friends, that Facebook had inadequate safeguards to protect user information, and that Facebook failed to be accountable for the user information under its control. The Commissioners made several recommendations that Facebook has either rejected or refused to implement. This matter is now before the Federal Court.

Full Disclosure: Political parties, campaign data, and voter consent (February 2019)

This comprehensive investigation evaluated how the BC NDP, Green, and Liberal parties manage personal information. The report found that the political parties are generally collecting too much information about potential voters without getting their consent. Sources of data include the electronic voters list from Elections BC, voter canvassing, data brokers, and social media. The investigation also found that consent should be obtained for the disclosure of email addresses to social media platforms for data analysis or profiling.

A total of 17 recommendations were made to improve the privacy practices of BC's main political parties. These included regular audits for all electronic systems containing personal information, employee and volunteer privacy training, retention periods for data, and amended privacy policies. Also recommended was a code of practice governing how political parties handle personal information when they accept the voters list from Elections BC. All three

political parties agreed to implement the recommendations, and our office is consulting with the parties on a code of practice.

Complaints

Individuals may make a complaint to the Commissioner with respect to an unauthorized collection, use, or disclosure of their personal information or with respect to their right of access or correction.

The OIPC receives approximately 200 complaints under PIPA from individuals on an annual basis. The majority of these are in relation to an unauthorized collection or disclosure.

The OIPC resolves most complaints through a mediation process. However, a small percentage proceed to inquiry where an adjudicator makes a finding regarding the application of PIPA and issues an order requiring an organization to address the complaint and meet its obligations under PIPA.

Privacy Breach Investigations

The OIPC investigated more than 100 privacy breaches during the last fiscal year. The number of privacy breach investigations has been increasing each year.

Audit and Compliance Program

The Audit and Compliance Program is responsible for conducting systemic investigations of public bodies and organizations either in response to a complaint or proactively. Audits with respect to organizations subject to PIPA in the past year included a compliance review of medical clinics and surveillance and compliance in a medical clinic.

Recent Orders and Court Decisions

One noteworthy order concerned an organization, known as “Surrey Creep Catcher”, which lured individuals to meet a decoy at a public space and then videotaped its confrontation with them and disseminated the video on social media. This vigilante-type operation was purportedly done to protect children from pedophiles and child predators. In response to complaints from two individuals, an investigation was done and concluded that the organization was not authorized to collect, use, and disclose personal information. Surrey Creep Catcher was ordered to stop these activities and to destroy all of the complainants’ personal information in its custody or under its control, and to ask others who disseminated the information to also destroy it.

Inter-jurisdictional collaboration

The OIPC regularly works with the Alberta and Federal Commissioners to share information and ensure a harmonized approach to private sector compliance. We have published joint guidance documents with these fellow regulators including a guide for organizations to develop privacy management programs and obtain meaningful consent from individuals.

The OIPC also conducts joint investigations with other Commissioners, most recently with the Privacy Commissioner of Canada investigating AggregateIQ and Facebook.

A Federal/Provincial/Territorial meeting of Commissioners is held annually for the purposes of information-sharing and discussing issues of joint concern. Commissioners issue a communique at the conclusion of the meeting advising the public of their common position with respect to immediate challenges in a priority area.

Recognizing that the flow of personal information crosses national borders means regulators must cooperate internationally to protect their citizens' data. BC business trades actively in the Asia Pacific region, meaning data flows follow. The OIPC plays a leading role as a member of the Asia Pacific Privacy Authorities (APPA) acting as the organization's secretariat with the Commissioner also serving as chair of APPA's Governance Committee.

The OIPC also acts as a coordinating force for the Global Privacy Enforcement Network (GPEN) hosting privacy experts to inform the work of GPEN in Australia, Hong Kong, Mexico and elsewhere.

THE NEED FOR REFORM

Previous Statutory Review (2014)

PIPA mandates a statutory review by a special committee of the Legislature every six years. Unfortunately, that prescient requirement for regular review of its effectiveness has not resulted in any improvements to the legislation. The last Special Committee made a number of critical recommendations for amendments to PIPA that, to date, have not been implemented. Those proposed amendments are needed even more now than they were in 2014.

We intend to make detailed recommendations to the Committee again in the fall. At that time, we will be endorsing some of those same recommendations from 2014 and make the case as to why they are urgently required as a matter of high priority. They include mandatory breach notification and the ability of the Commissioner to impose administrative monetary penalties.

Another significant recommendation made by the previous Committee was for a new stand-alone health information privacy law in British Columbia. Government has indicated that it is prepared to proceed with this legislative initiative. In that event, it is anticipated that

amendments will be required to PIPA to carve out professional regulatory bodies and private practices of health professionals (including physicians' offices) from its scope of application.

We submit that a major reform of PIPA should proceed in advance of a brand-new piece of privacy legislation in the Province for the health sector. This would help to ensure that both pieces of privacy law are on par and consistent. British Columbians should have important privacy rights with respect to their sensitive personal health information; there should be a level playing field for health care organizations and other organizations in terms of their privacy obligations, and the Commissioner should have the same abilities to exercise proper oversight.

Keeping Pace with National and International Trends

Fundamentally, PIPA is principles-based and technology neutral. It is therefore flexible and its general conceptual structure works for all types and manners of collection, use, and disclosure. In this sense its general framework is a sound one. Another virtue is its broad scope of application. In particular, it is unique in Canada in that it applies to political parties.

However, in most other respects PIPA has failed to keep pace with changes of the past 17 years. Only minor consequential amendments have been made to PIPA since it was adopted in 2003. While PIPA was considered a modern piece of legislation at that time, it now has glaring gaps and omissions. Major reform is urgently needed. Compared to other jurisdictions, British Columbians have a lesser standard of privacy rights, organizations in British Columbia have fewer privacy obligations, and the Commissioner lacks tools to properly enforce the Act effectively.

The new General Data Protection Regulation (GDPR) in the EU and its influence globally cannot be ignored. It has become a gold standard and a model for many jurisdictions around the world. In particular, the GDPR confers such privacy rights as the right to erasure (right to be forgotten), the right to data portability, and the right to object to data processing activities. Issues around individual privacy rights will have to be examined by the Committee.

Commissioner's Recommendations

The Commissioner's submission to the Committee in the fall will make recommendations in considerable detail to clarify, strengthen, and enhance PIPA. However, we wish to take this opportunity to highlight our three most pressing concerns.

The Serious Need for Mandatory Breach Reporting

Surprisingly, PIPA does not require an organization to notify our office or affected members of the public when there has been a significant unauthorized disclosure of personal information. These serious breaches of privacy, often impacting thousands of individuals, occur for any number of reasons including cyberthreats, theft of mobile devices, and employee error or snooping.

Unless an organization voluntarily reports to us, we do not know if those affected by a serious breach have been notified, or whether the organization has remedied the cause of the breach to prevent recurrence. This is a significant risk to the privacy of British Columbians because they may not be aware that they need to take steps to mitigate the risk of financial or other harm caused by the improper disclosure of their personal information. There are also lost opportunities for the Commissioner to educate organizations on how to improve their privacy controls.

Both Alberta and Federal private sector privacy laws were amended to require organizations to notify Commissioners' offices of significant privacy breaches. Mandatory breach notification exists in almost all states in the US and is in the GDPR. It is well-recognized as an essential tool that every privacy regulator needs in their toolbox to exercise proper oversight.

The Ability to Levy Administrative Monetary Penalties

It is essential that the Commissioner be given the authority to levy administrative monetary penalties against bad actors who transgress the law. It is no longer sufficient to "name and shame" these organizations into compliance. Fines will incentivize compliance. It is also important that they be set at substantial levels so that they do not simply become a cost of doing business. It should be noted that the Commissioner already exercises this authority to impose fines in relation to non-compliance with the BC *Lobbyists Transparency Act*.

A recent investigation of Facebook by the Federal Competition Bureau resulted in a settlement agreement for $9.5 million. The Competition Bureau found that Facebook made false or misleading claims about the disclosure of personal information on Facebook or Messenger. In contrast the OIPC could levy no penalty against Facebook despite the fact that its joint investigation with the OPC found that, among other things, Facebook inadequately safeguarded user information.

Conducting Investigations

The Commissioner's inability to issue an order where an investigation has been initiated without a complaint is a serious omission that needs to be rectified. Such investigations are increasingly important because of the opacity with which (especially technology companies) process personal information. 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. This increasing power imbalance between consumer and commercial organizations can be rectified by ensuring the Commissioner's ability to initiate investigations and make orders that protect consumers. The Commissioner already has this authority in relation to public sector privacy under the *Freedom of Information and Protection of Privacy Act*.

Further details with respect to each of these matters and others will follow in our forthcoming fall submission.

CONCLUSION

The convening of this Committee comes at a critical juncture. The escalation of technological developments increasingly compels us to consider how much we value our privacy. As our submission makes clear, and we hope you agree, the laws governing the collection and use of personal information in this changing environment are in urgent need of reform. Citizens must be able to confidently navigate their digital world, and businesses allowed to operate on a well-regulated playing field that benefits companies who act in accordance with consumer expectations and penalize those that don't. The trend to global privacy law reform is not limited to Europe. Many of the principles of GDPR have been embraced from California to Japan. British Columbia must pay heed to global currents for both the benefit of our citizens and for businesses that market themselves within BC and across the world.

We are very pleased that the Committee is engaging in a public consultation process and will be receiving input from a wide cross-section of individuals, organizations, and other stakeholders. We intend to closely monitor the progress of the statutory review and our more comprehensive submission in the fall will include comments on other submissions to the Committee.

We are at the disposal of the Committee during the conduct of its statutory review and would be happy to provide further information or materials as needed.

We are hopeful that reforms recommended by the Committee at the conclusion of this review will be seriously considered by government and will result in the introduction of proposed amendments in the Legislative Assembly for Members' consideration at the earliest opportunity. The time for reform is now.

June 2, 2020

ORIGINAL SIGNED BY

Michael McEvoy
Information and Privacy Commissioner
for British Columbia

APPENDIX

PrivacyRight: Fundamentals for business (2019)
Major public education program consisting of a series of animated webinars, videos, and podcasts that explain the basic obligations of organizations under PIPA. They include information about establishing a privacy management program and how to respond to an access request.

Collecting personal information at food and drink establishments during Covid-19 (May 2020)
How to collect contact information for the purposes of contact tracing in a privacy protective manner.

Tips for public bodies and organizations setting up remote workplaces (March 2020)
This timely guidance was prepared because of the large number of employees who began working from home in the wake of the outbreak of Covid-19.

Privacy Impact Assessment Template (January 2020)
Privacy Impact Assessments for the Private Sector (January 2020)
Companion documents that guide organizations through the process of preparing a comprehensive privacy impact assessment on a proactive basis with respect to new initiatives in order to identify privacy risks, impacts, and necessary mitigation strategies.

Responding to PIPA Privacy Complaints (October 2019)
Three steps that organizations should take when they receive a privacy complaint.

Private sector landlords and tenants (September 2019)
Helps landlords and the public understand what personal information landlords may collect from a prospective tenant.

Privacy-proofing your retail business: FAQs and tips for protecting customers' personal information (June 2019)
How PIPA applies to situations commonly faced by retail organizations in their consumer transactions.

Developing a privacy policy under PIPA (March 2019)
Key elements of privacy policies and practices within organizations.

Privacy Management Program Self-Assessment (March 2019)
Checklist that can be completed voluntarily and returned to the OIPC on a strictly confidential basis for additional information or assistance.

Competitive Advantage: Compliance with PIPA and the GDPR (March 2018)
This guidance document was published prior to the GDPR coming into force in order to inform organizations of new privacy requirements they will have to meet to continue to do business in Europe and the UK.

Obtaining Meaningful Consent (May 2018)
Joint publication with the Alberta and Federal Commissioners offering practical and actionable guidance on what organizations should do to ensure they obtain meaningful consent for the collection, use, and disclosure of personal information. It sets out seven guiding principles and includes a checklist.

Protecting Personal Information: Cannabis Transactions (October 2018)
Helps cannabis retailers and purchasers understand their rights and obligations under PIPA.

Guide to Using Overt Video Surveillance (October 2017)
This guidance was released at the same time as the results of an audit of video surveillance at a medical clinic.

Guide to OIPC Processes - PIPA (May 2017)
How the OIPC responds to complaints made under PIPA.

BC Physician Privacy Toolkit 3rd edition (November 2017)
The Toolkit is a joint publication of the OIPC, the College of Physicians and Surgeons of BC and Doctors of BC and gives guidance to physicians in private practice on how best to meet their obligations under PIPA.

Privacy Guidelines for strata corporations and strata agents (June 2015)
PIPA and Strata Corporations: FAQs (June 2015)
Comprehensive information for strata councils and strata owners about what personal information can be collected, used, and disclosed under PIPA for the purposes of managing a strata building.

The Commissioner and staff also make presentations at workshops, meetings and conferences regarding PIPA compliance throughout the year. Guidance documents can be viewed at https://www.oipc.bc.ca/resources/guidance-documents/.