Office of the
Privacy Commissioner
of Canada

PRIVACY LAW REFORM

A PATHWAY TO RESPECTING RIGHTS AND RESTORING TRUST IN GOVERNMENT AND THE DIGITAL ECONOMY

2018 • 2019
ANNUAL REPORT

2018-2019 Annual Report to Parliament on the *Privacy Act*
and the *Personal Information Protection and Electronic Documents Act*

Office of the Privacy Commissioner of Canada
30 Victoria Street
Gatineau, Quebec K1A 1H3

Cat. No. IP-1E-PDF
ISSN 1913-3367

Table of contents

Commissioner's message

For several years, my predecessors and I have been calling for fundamental reform of Canada's federal private and public sector privacy laws. In the last year, the government has finally agreed the time for reform had come. Members of the Standing Committee on Access to Information, Privacy and Ethics (ETHI), from all parties, also agree. Even big tech companies proclaim that the age of self-regulation is over. The question is no longer whether privacy laws should be modernized, but how.

Privacy is a concept that is contextual and sometimes difficult to define precisely, but it is nevertheless a foundational value in Canadian society, a fundamental right and, as we have seen in the recent Cambridge Analytica scandal, a prior condition to the exercise of other fundamental rights, including freedom, equality and democracy. The starting point, therefore, should be to give new privacy laws a rights-based foundation.

Data-driven technologies undoubtedly bring great benefits to individuals. They can be fun and convenient, but, on a more fundamental level, they can also be powerful tools for personal development. They also open the door to huge opportunities for improving health care, the environment and economic growth.

On the other hand, these technologies create new risks. For good and bad, they are a disruptive force.

Apple's Tim Cook warned last year that a "data industrial complex" is being formed where "our own information, from the everyday to the deeply personal, is being weaponized against us with military efficiency." He added: "This is surveillance." American researcher Shoshana Zuboff similarly describes the new economic model as surveillance capitalism. Canadian artificial intelligence expert Yoshua Bengio argues that "the only way to restore balance is to ensure that individuals are not left alone when interacting with businesses. What is the role of governments if not to protect individuals?"

While new privacy laws should allow for responsible innovation, I agree wholeheartedly that individuals should not be left alone when interacting with businesses. Privacy is often seen through the lens of website terms and conditions leading to a less than meaningful form of consent, but this is a narrow view, and one which puts individuals at a distinct disadvantage when faced with organizations with immeasurably more knowledge and power.

Technical rules in place to protect personal data, such as consent, access and transparency, are important mechanisms for the protection of privacy, but they do not define the right itself.

Legislation should define privacy in its broadest and true sense, for instance, by describing it as freedom from unjustified surveillance. Canadians want to enjoy the benefits of digital technologies, but they want to do it safely. Legislation should recognize and protect their freedom to live and develop independently as persons, away from the watchful eye of a surveillance state or commercial enterprises, while still participating voluntarily and safely in the regular, day-to-day activities of a modern digital society.

While there is general agreement that legislative reform is needed, we continue to hear industry and government officials adopting language that emphasizes the need to balance privacy rights with economic interests, security and other important goals. They imply that privacy and objectives such as innovation are engaged in what some have called a zero-sum game.

We must reject the notion that rights-based laws impede economic growth or other important societal objectives. Fundamental rights are not an impediment to innovation or the delivery of government services in the digital age. In fact, a rights-based statute would serve to support responsible innovation by promoting trust in government and commercial activities.

It is not an exaggeration to say that the digitization of so much of our lives is reshaping humanity. If we are not careful, it will be reshaped in ways that do not accord with our most fundamental rights and values. Therefore, uses of technology that are incompatible with these rights and values should not be permitted. The market has proven time and again that it is creative; it will find profitable ways to offer products and services that meet genuine needs while respecting new laws that are based on rights and values. The same should be true of democratic governments subject to the rule of law.

We have devoted a chapter of this annual report to exploring a number of issues related to law reform, including how a rights-based approach for protecting Canadians' privacy could be effectively implemented. Let me highlight here a few of the most important features of that approach.

First, the law should be able to endure over time, meaning it should remain relevant despite technological changes. The pace of technological developments is exponential and it is simply not possible for the law to be amended at the same speed. This is an argument advanced by industry and government for a principles-based legislation, but it also lends support for a law that defines privacy in its broadest and true sense. Technical protections, such as defining what information is required for meaningful consent, are often ineffective as they are regularly overtaken by developments in technology. However, the values that underpin the right to privacy are unlikely to change significantly over time. Defining privacy in its full sense, in accordance with its underlying values, would ensure it continues to be protected, regardless of technological changes.

It is not an exaggeration to say that the digitization of so much of our lives is reshaping humanity. If we are not careful, it will be reshaped in ways that do not accord with our most fundamental rights and values.

Second, in the private sector, the law should truly and firmly put an end to self-regulation. This means, in part, that there should be an ability for a public authority to prescribe subsidiary binding rules, giving effect to the principles in specific contexts, so that both individuals and commercial and state organizations have some certainty as to their rights and obligations.

The public authority could be either my Office, a government department or some other emanation of the state. Industry codes and ethical rules have their place, they can increase transparency and consistency, but they are not legally binding nor enforceable and cannot replace state-made rules adopted in the public interest. Without binding subsidiary rules, organizations have too much discretion to apply principles as they see fit, sometimes making these principles hollow. This amounts to self-regulation, and the past few years have shown the risks and limits of that approach.

What is required is a law that ensures demonstrable accountability, meaning accountability that is demonstrated to the regulator, an independent third party.

Another form of self-regulation would remain if the accountability principle included in the *Personal Information Protection and Electronic Documents Act* (PIPEDA) were to be maintained in its current form or given an enhanced role. The business community has championed accountability as an important component of privacy protection. Industry argues accountability should be given even more importance, as it says, rightly, that consent is increasingly ineffective in protecting privacy. I agree accountability is important. However, as we have so clearly seen in Facebook, Equifax and other cases, the principle as currently framed is not sufficient to protect Canadians from the practices of companies that claim to be accountable, but actually are not.

What is required is a law that ensures demonstrable accountability, meaning accountability that is demonstrated to the regulator, an independent third party. In today's world where business models are opaque and information flows are increasingly complex, individuals are unlikely to file a complaint when they are unaware of a practice that may harm them. This is why it is so important for the regulator to have the authority to proactively inspect the practices of organizations. Where consent is not practical and organizations are expected to fill the protective void through accountability, these organizations must be required to demonstrate true accountability upon request.

Demonstrable accountability is also part of the solution in protecting Canadians in the context of transborder data flows. I recognize these data flows are the subject of international trade agreements and bring important benefits to individuals and organizations. But I also firmly believe that government has an obligation to protect the privacy of its citizens through the adoption of effective privacy laws. Our Equifax investigation has proven that PIPEDA's accountability principle is not always effective in protecting Canadians in the context of international transfers. The law must be strengthened, at least through the adoption of demonstrable accountability, and possibly other means, such as adopting the European regime of standard contractual clauses.

As a third key element of a rights-based approach to legislative reform, in the public sector, the law should adopt the principles of necessity and proportionality. Digital technologies have made it much easier for government to collect, share, use and store the personal information of individuals. The shift from paper-based to digital format records has actually led to a dynamic of over-collection. Our Statistics Canada investigation underscored how over-collection of personal information without appropriate consideration of necessity and proportionality can be extremely intrusive. It would be more in keeping with the quasi-constitutional status of the *Privacy Act* if personal information collection

by government was explicitly limited to those elements demonstrably necessary for operation of a program or activity and proportional to the privacy risks. Almost all of the provinces and territories have set necessity as a standard, as have many member economies of the Organization for Economic Co-operation and Development (OECD). Federal legislation should adopt the same threshold to reflect modern reality and expectations.

Fourth and finally, the law should provide for enforcement mechanisms that ensure individuals have access to a quick and effective remedy for the protection of their privacy rights, and that create incentives for broad compliance at all times by federal institutions and commercial organizations.

Canada's laws have unfortunately fallen significantly behind those of trading partners in terms of the enforcement of privacy laws. At the same time, most Canadians believe their privacy rights are not respected by organizations. This is a damning condemnation, and, in my view, an untenable situation in a country governed by the rule of law. It is certainly not conducive to building consumer trust, one of the government's stated objectives.

The government's Digital Charter suggests that my Office should be granted "circumscribed" order-making powers and that before fines are imposed for violations of the law I have identified following an investigation, I should first convince the Attorney General to further investigate and eventually bring the matter before a judge. By contrast, my EU and US equivalents, among others, can directly order companies to comply with the law and can order sizeable fines, subject of course to judicial review. In my view, the government's proposal is very inefficient, given it would seriously delay the enjoyment of rights by individuals to several years after they have filed a complaint. Justice delayed is justice denied.

True order-making powers and fines would change the dynamic of our discussions with companies during investigations, leading to quicker resolutions for Canadians. At the moment, as we saw in our Facebook investigation, an organization that we have found in contravention of the law can simply ignore our recommendations and "wait it out" until the courts have come to the same conclusion as my Office. In the government's proposal under the Digital Charter, a further step would be added, in the form of a review by the Attorney General.

Both the current framework and the government's proposal create an excellent incentive for companies not to take privacy seriously, change their practices only if forced to after years of litigation, and generally proceed without much concern for compliance with privacy laws. My fellow privacy commissioners at both the provincial and international levels who have already been empowered to make orders and impose fines report that these enforcement tools have led to much more cooperation from companies. When the regulator finds a violation, companies are more willing to correct deficiencies, without long delays.

Ultimately, enforcement mechanisms should result in quick and effective remedies for individuals, and broad and ongoing compliance by organizations and institutions. Only then will trust in the digital practices of companies and government reach the levels we all want.

Privacy by the numbers

1,420
Privacy Act complaints accepted

380
PIPEDA complaints accepted

315
PIPEDA data breach reports examined

433
Privacy Act complaints closed through early resolution

178
PIPEDA complaints closed through early resolution

21
Advisory engagements with businesses

933
Privacy Act complaints closed through standard investigation

104
PIPEDA complaints closed through standard investigation

23
Bills, legislation and parliamentary studies reviewed for privacy implication

155
Privacy Act data breach reports examined

87
Advice provided to public sector organizations following PIA review or consultation

14
Formal briefs submitted to Parliament on private and public sector matters

56
News releases and announcements

76
Privacy impact assessments (PIAs) received

383
Public interest disclosures by federal organizations

10,200
Information requests

1,098
Tweets sent

48
Advisory consultations with government

16
Parliamentary committee appearances on private and public sector matters

75
Speeches and presentations

15,301
Twitter followers

2,808,560
Visits to website

208,282
Blog visits

45,598
Publications distributed

Advice to Parliament

Privacy Law Reform: A Pathway to Respecting Rights and Restoring Trust in Government and the Digital Economy

Introduction

In our last three Annual Reports, our Office has provided a detailed account to Parliament that Canadians need stronger, more enforceable, federal privacy laws. The backdrop of events prompting this need for law reform is the rapid growth of information technologies pervading the economy and government alike. The digital age that is before us is one that is increasingly predicated on mass data collection and sharing, automated decision-making, and profiling. The privacy implications and, by extension, risks to fundamental rights and freedoms, are immense.

In recent time, the Government of Canada has also recognized that the time has come to improve our privacy laws. In this regard, the Standing Committee on Access to Information, Privacy and Ethics (ETHI) issued a report on their review of the *Privacy Act* in December 2016, to which the government responded by committing to launch its own review toward modernizing the Act. Likewise, ETHI issued a report on its review of PIPEDA in February 2018. The Government agreed with ETHI that changes were required to Canada's private sector privacy regime to "ensure that rules for the use of personal information in a commercial context are clear and enforceable and will support the level of privacy protection that Canadians expect."

Most recently, ETHI issued a report, *Democracy under Threat: Risks and Solutions In The Era of Disinformation and Data Monopoly,* which provided the government a number of recommendations meant to address self-regulation of platform monopolies and associated vulnerabilities to our democratic and electoral processes due to improper acquisition and manipulation of personal information. In its response to this ETHI report, the Government echoed once again that Canada's privacy regime must be updated with clear and enforceable rules to protect Canadians' privacy.

Shortly after the Government's response to this ETHI report, Innovation, Science and Economic Development Canada (ISED) published a proposal to modernize PIPEDA, and Justice Canada released a plan to engage stakeholders on modernizing the *Privacy Act*.

Further reading

ETHI, Protecting the Privacy of Canadians: Review of the *Privacy Act*, December 2016

Government of Canada's Response to Protecting the Privacy of Canadians: Review of the *Privacy Act*, April 2017

ETHI, Towards Privacy by Design: Review of the *Personal Information Protection and Electronic Documents Act*, February 2018

Government of Canada's Response to Towards Privacy by Design: Review of the *Personal Information Protection and Electronic Documents Act*, June 2018

ETHI, Democracy under Threat: Risks and Solutions in the Era of Disinformation and Data Monopoly, December 2018

Government of Canada's response to Democracy under Threat, Risks and Solutions in the Era of Disinformation and Data Monopoly, January 2019

ISED, Strengthening Privacy for the Digital Age, May 2019

Department of Justice, Modernizing Canada's *Privacy Act*, August 2019

Internationally, privacy laws in several jurisdictions have been strengthened to address privacy challenges in a digital age. It is clear that privacy reform is gaining momentum on the global stage, as governments and legislators around the world have come to realize the shortcomings and threats of self-regulation models in a globalized digital economy. It is our hope that Canada is ready to take firm, decisive action to modernize our privacy laws to better protect the rights of Canadians as they interact with businesses and government in this increasingly digital world in which personal information has become a primary currency.

To be clear, we recognize that the digital age has engendered better services, whether it be services delivered by governments to citizens or companies to consumers. The digital age has inspired creativity in the way businesses and governments work, and in the way individuals socialize and communicate. Digital services are being developed to benefit society in all sorts of ways, from new health devices, to technologies aimed at environmental protection. Such innovation is vital for Canada's continued economic growth, and having a strong legislative framework that positions Canada as a privacy leader will only serve to strengthen our competitive position.

Our view is that Canada's federal privacy laws should remain technology-neutral and principles-based, as these elements will enable the law to provide a level-playing field across industry sectors and to endure over time, that is, remain relevant despite the exponential pace of technological change. The rapid development of new technologies will require legislative amendments from time to time, meaning there should be periodic reviews of our privacy laws, potentially every five years or so, but the principles-based nature of the law should result in continued relevance without requiring constant revisions to keep pace.

At the same time, we believe that Canadians also deserve federal privacy laws that are based on rights for individuals. The incorporation of a rights-based framework in our privacy laws would help support responsible innovation and foster trust in government, giving individuals the confidence to fully participate in the digital age. We are certain that both private and public sector organizations will be able to continue to innovate and thrive in an environment that both supports and encourages innovation and recognizes and protects the privacy rights of individuals. In fact, a greater focus on privacy rights, responsible practices, and transparency could assist the business community and public sector in ensuring that they remain competitive and relevant on both a domestic and international level given global developments in this regard.

In this chapter, we will outline what we mean by a rights-based approach for protecting Canadians' privacy. We will explain possible options for bringing federal privacy laws into the 21st century. Finally, we will conclude with a broad discussion of a number of key elements that we suggest are fundamental for privacy law reform in Canada.

Recognizing privacy as a human right

At its core, privacy is a cherished Canadian value that is deeply rooted in a tradition of human rights.

Since as early as 1948, Canada recognized and signed a number of seminal international human rights agreements that firmly entrenched privacy as a fundamental right to human dignity and integrity, to one's honour and reputation, and which afforded protection against arbitrary interference into one's private life or communications. In 1968, Parliament's Standing Committee on Justice and Legal Affairs began to call on the government to create privacy legislation. Following discussions at the Canadian Bar Association's meeting of that year, the federal Department of Justice began to work on a draft privacy bill. These efforts culminated in Canada's first statutory privacy protective measures applicable to actions of the federal public sector, enacted under the anti-discrimination provisions in Part IV of the *Canadian Human Rights Act* in 1977, followed by the promulgation of the *Privacy Act* in 1983.

Further reading

Bill S-21, *An Act to guarantee the human right to privacy*, 2001

Supreme Court of Canada, *R. v. Spencer*, 2014

Supreme Court of Canada, *R. v. Jones*, 2017

Supreme Court of Canada, *R. v. Jarvis*, 2019

41st International Conference of Data Protection and Privacy Commissioners, *International resolution on privacy as a fundamental human right and precondition for exercising other fundamental rights*, 2019

There have also been attempts at the federal level to bolster and further formalize the human right to privacy protection. In 2000, Senator Sheila Finestone introduced Bill S-21, an *Act to guarantee the human right to privacy* ("the Finestone Charter") in the Canadian Senate. This Bill attempted to situate privacy within the broader human rights framework, and thus, to facilitate the interpretation of privacy obligations in a broader sense. The Finestone Charter defined the right to privacy as including physical privacy, freedom from surveillance, freedom from monitoring and interception, and freedom from collection, use, and disclosure of personal information.

Since the time of the Finestone Charter, the Supreme Court of Canada has developed and refined its understanding of privacy and applied

it in a diverse range of contexts. This has included, but not been limited to, the discrete list of activities that the Finestone Charter sought to protect. In *R v Spencer*, the Supreme Court of Canada recognized privacy to include the notion of secrecy or confidentiality; control over, access to and use of information; and anonymity. More recently, in *R v Jarvis*, the Supreme Court of Canada confirmed that privacy is not an "all-or-nothing concept", and that being in a public or semi-public place does not negate all expectations of privacy with respect to being observed or recorded.

The Supreme Court of Canada has also repeatedly recognized privacy as necessary for the realization of other human rights protected under the *Canadian Charter of Rights and Freedoms* ("*Charter*"), and has affirmed the quasi-constitutional status of both federal and provincial privacy legislation. In *R v Jones*, the Supreme Court of Canada also recognized that personal privacy is vital to an individual's dignity, autonomy, and personal growth, and accordingly, that the protection of personal privacy is a basic prerequisite to the flourishing of a free and healthy democracy.

Despite this tradition of privacy being recognized as a fundamental human right necessary for the exercise of other rights, our current privacy laws are drafted largely as data protection statutes rather than as laws that protect and promote the exercise of a broad range of rights. Privacy is not limited to consent, access and transparency. These are important mechanisms, but they do not define the right itself nor acknowledge its quasi-constitutional status. Our laws must be reframed to recognize that privacy is nothing less than a prerequisite for freedom: the freedom to live and develop independently as individuals, away from the watchful eye of surveillance by the state or commercial enterprises, while participating fully in the regular, day-to-day activities of a modern society. This sentiment is echoed by the international data protection and privacy commissioner community as reflected in its recent *International resolution on privacy as a fundamental human right and precondition for exercising other fundamental rights*, adopted at the 41st International Conference of Data Protection and Privacy Commissioners in October 2019.

While times are much different now than in 2000, when Senator Finestone introduced her Charter, it is clear that the right to privacy remains worthy of statutory protection. Modernized privacy legislation should start by defining privacy in its proper breadth and more formally codify its quasi-constitutional status. This, alongside the principles-based and technology neutral nature of the law, would ensure our law can endure over time, be interoperable with the laws of other jurisdictions, and also be reflective of Canadian values.

A rights-based approach for protecting Canadians' privacy

As mentioned, currently Canada's federal privacy laws are narrowly framed as data protection statutes. PIPEDA and the *Privacy Act* codify a set of rules for how organizations and federal government institutions are required to handle an individual's personal information. Although under both laws, individuals have a right to access and correct their personal information, and the right to file a complaint with our Office, neither law formally recognizes privacy as a right in and of itself. Privacy is broader than data protection, although the latter seeks to participate in the protection of the former. If our data protection laws are to more meaningfully protect the broader right to privacy, this goal needs to be reflected more explicitly in the formulation of our data protection statutes.

Many international instruments that were recently adopted or revised have already taken steps in this direction, though there remains a lack of harmonization in this regard. For example, the EU's *General Data Protection Regulation* (GDPR) has incorporated a human rights-based approach to privacy within its data protection legislation. Throughout 173 recitals, the GDPR makes repeated references to fundamental rights of individuals in relation to data processing. For example, the second recital states that: "The principles of and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms". As noted in Dr. Teresa Scassa's paper, "A Rights-Based Approach to Data Protection in Canada" (2019), embedding human rights within the GDPR has the advantage of making newer, more modernized rights easier to reconcile than within a narrow conception of data protection. She notes for example, the right to be forgotten is not simply a right to control one's personal information but can also be linked to a right to develop as a person, allowing us to experiment, make mistakes and start afresh in an online environment. This goes beyond simple data protection and implicates a human right to privacy.

Further reading

EU *General Data Protection Regulation*

Summary of Privacy Laws in Canada

Provincial legislation deemed substantially similar to PIPEDA

Report of findings: Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia

To be clear, we are not suggesting that other kinds of privacy protections do not exist elsewhere in Canadian law. There are several laws in Canada that relate to privacy, and enforcement of these laws is handled by various levels of government and courts. As alluded to above, courts have relied upon section 7 (the right to life, liberty and security of the person), and section 8 (the right to be secure against unreasonable search and seizure) of the *Charter* to protect individuals against unreasonable invasions of their privacy by the state.

As in the case of human rights more generally, privacy is not exclusively a matter of federal jurisdiction in Canada. There are privacy laws that apply to provincial government activities, and several provincial statutes have been deemed substantially similar to PIPEDA. In many ways, these provincial privacy laws offer stronger privacy protections than our federal statutes.

Amid this complex environment of context-specific privacy protections dispersed throughout varying jurisdictions, and set against a backdrop of accelerated growth in the data economy, it would be useful for the federal government to recognize more comprehensively the privacy rights afforded to individuals. Doing so would give public and private organizations more clarity as to their obligations for protecting individuals' privacy rights and individuals more certainty in their ability to both exercise and enforce their rights.

We are proposing that both of our federal privacy laws be amended to be given a rights-based foundation that recognizes privacy in its proper breadth and scope, and provides direction on how the rest of the acts' provisions should be interpreted. This direction could take a form similar to the supplement found at the end of this chapter.

We also propose that rights-based legislation contain the following key elements:

1) **Define the right to privacy in its broadest sense**, which means to make explicit that a central purpose of the law should be to protect privacy as a human right in and of itself, and as essential for the realization and protection of other human rights. A broad definition of privacy, consistent with the Finestone Charter, could include "freedom from surveillance, without justification", these last two words confirming that privacy is not an absolute right. Finally, a definition of privacy as a right would be reflective of the rich jurisprudence on this subject, including by the Supreme Court of Canada.

2) **Recognize in law the quasi-constitutional nature of privacy legislation**, which means confirming the protected status of privacy as established through decisions of the Supreme Court of Canada, where the Court recognized the fundamental role privacy plays in the preservation of a free and democratic society.

3) **Draft the law in the usual manner of legislation, conferring rights and imposing obligations**, rather than as the current model, which contains what reads as an industry code of conduct, with some obligations but also several recommendations, examples and good practices that do not create enforceable entitlements for individuals. Courts have also noted that, due to its non-legal drafting, PIPEDA is not an easily accessible statute and gives little, if any guidance at all, to those who must interpret it.

4) **Ensure effective enforcement**, which means adopting enforcement mechanisms that would result in quick and effective remedies for individuals, and broad and ongoing compliance for organizations and institutions. Without effective enforcement, rights become hollow and trust dissipates.

Among the improvements required is to empower the Privacy Commissioner of Canada to conduct proactive inspections, make binding orders and impose consequential penalties for non-compliance with the law. Proactive inspections are discussed in more detail later in this chapter in relation to demonstrable accountability. Such inspections are necessary to ensure ongoing compliance with the law, in contrast with the current system where violations have first to be identified (not an easy task in this digital age), then investigated and, ultimately, voluntarily remedied by an organization, for compliance with the law to finally be restored. Proactive inspections, combined with order making and fines, would serve to encourage ongoing compliance and thus greatly enhance consumer trust.

In other jurisdictions within Canada and abroad, privacy or data protection regulators have the authority to issue binding orders and fines, subject to judicial review. Giving these powers to a first level authority rather than requiring individuals to wait until a court, several years after an alleged violation, upholds a complaint, is a much more effective way to ensure the timely enjoyment of rights. Again, this is the legislative model followed by several Canadian provinces, as well as by a number of Canada's trading partners, including the US and the EU. All Canadians deserve to have their privacy rights enforced as effectively as in comparable jurisdictions.

While greater powers for the Office of the Privacy Commissioner (OPC) are part of the solution, they are not the only one from an enforcement perspective. With finite resources and a multitude of roles and responsibilities, the OPC cannot investigate every violation of the law. In a rights-based model, it is important that individuals have an independent right of action in the courts to seek remedies for non-compliance with their rights.

Events of this past year have highlighted like never before the urgent need to modernize the way in which privacy rights are protected in this country. To give but one example, our Facebook investigation found that the company committed serious contraventions of Canadian privacy laws in the wake of revelations about the company's disclosure of the personal information pertaining to some of its users to a third-party application, which was later used by third-parties for targeted political messaging. In response to our investigative findings, Facebook disputed what we found; refused to address the serious problems we identified; and would not acknowledge that it broke the law.

This situation highlights serious weaknesses with our current privacy protection framework. For a company like Facebook to dismiss the investigative findings of our Office and think it can decide what legal obligations it will or will not follow is untenable. Canada requires updated privacy laws that provide for effective enforcement and recourse, and that consider privacy in its full spectrum of rights. Such a reformulation of our privacy laws will help to restore trust in Canadian democracy and our economy.

Additional elements for privacy law reform in Canada

In addition to a reframing to incorporate a rights-based framework, our Office is currently assessing additional elements that would be fundamental to modernizing our privacy laws. Informing our work is the Office's compliance, policy and advisory files, legislative modernization occurring internationally, and specific proposals for law reform put forth by both Innovation, Science and Economic Development (ISED) as well as Justice Canada, among other considerations.

The following is an overview of some key issues that we are currently exploring from a policy perspective relating to legislative modernization. Specifically, we believe that Canadian privacy laws need to be updated to:

1) Maintain an important place for meaningful consent, but also include alternative solutions to protect privacy where consent is not feasible.

The principle of consent under PIPEDA relates to individual autonomy, allowing one to exercise some level of control in the handling of their data. Consent can play an important part in protecting privacy. Yet, the limits of consent are increasingly apparent in an environment where innovation and profit generation can motivate some to use data for purposes other than those for which it has been collected. Individuals are now faced with an excessive burden and an unreasonable shift in accountability, due to vague and unintelligible consent requests.

When it comes to the federal government's collection of personal information under the *Privacy Act*, the obligation to obtain an individual's consent is much narrower than it is in PIPEDA. Rather, under the *Privacy Act*, a federal government institution is entitled to collect and use one's personal information without consent so long as the information relates directly to the institution's operating program or activity. Obtaining consent from an individual is only required when a federal government institution uses or discloses personal information beyond its stated purpose or permitted exceptions under the Act.

We hold the view that there should still be a place in the law for consent, where it is an effective means for individuals to exercise control over their information. When consent is sought from individuals, it must also be meaningful. In our 2018 *Guidelines for obtaining meaningful consent*, which focused on PIPEDA, we highlighted a number of ways to ensure that consent from the individual to collect, use or disclose their personal

data is meaningful. To give but just a few examples, we saw it necessary for private organizations to:

- Provide individuals more accessible and easy to understand descriptions about the information collected. This should also include specifying with whom the data is being shared; for what purposes it will be collected, used and disclosed; and what uses are not essential for providing the service. Finally, individuals should be made aware of any meaningful risks of harm in using the services provided.
- Allow individuals to control the level of detail they get from the organization and when.
- Design and/or adopt innovative consent processes that can be implemented just in time, are specific to the context and appropriate to the type of interface used.

While there still is a place in the law for requiring an individual's consent, exceptions to consent should perhaps be permitted under specific circumstances defined in legislation where the societal benefits clearly outweigh the privacy incursions and several prior conditions are met before information is used for such purposes. Societal benefits have also been referred to by some as "socially beneficial purpose" or "public good". We are of the view that there has to be a more critical examination of what companies (and governments) believe to be societal benefits. We have learned through our investigative and advisory work that purported socially beneficial uses by a company, industry or government are not always in alignment with the public's idea of societal good or individual interests – some benefits are greater than others, and there are limits to how much individuals are willing to compromise their rights in the name of the public good.

In the Report on Consent included in our 2016-2017 Annual Report, we proposed that Parliament consider amending PIPEDA to introduce new exceptions to consent to allow for socially beneficial activities that the original PIPEDA drafters did not envisage. We suggested that any private sector organization wanting to exercise such an exception would need to meet several prior conditions, including that:

- it is necessary to use personal information;
- it is impracticable to obtain consent;
- pseudonymized data will be used to the extent possible;
- societal benefits clearly outweigh any privacy incursions;
- a privacy impact assessment (PIA) was conducted in advance;
- the organization has notified the OPC in advance;
- the organization has issued a public notice describing its practices; and
- individuals retain the right to object.

Under the GDPR, there are a number of lawful bases for processing personal information, one of which is for a "legitimate interest". In order to rely on the legitimate interest provision, an organization must first explain the purpose and demonstrate the necessity of the processing, and further justify that the organization's interests do not infringe upon individuals' interests, rights or freedoms. Moreover, organizations relying on legitimate interests are required to consider individual objections. In some limited instances, public authorities are able to consider using legitimate interests as a lawful basis for processing; however, it is likely that other lawful bases (i.e. their legal mandates) would be more appropriate.

In its paper, *Strengthening Privacy for the Digital Age,* ISED notes that it is exploring how exceptions to consent could look under a modernized law through its proposed concept of "standard business practices". They outline that this could

capture purposes such as fulfilling a service; using information for authentication purposes; sharing information with third-party processors; risk management; or meeting regulatory requirements. As currently described, "standard business practices" as proposed by ISED is too broad of a concept, one that risks becoming a catch-all exception, if not a gaping hole. Put simply, businesses should not be allowed to dispense with consent merely because a practice is one they determine to be "standard".

For its part, Justice Canada is considering the appropriate role of consent under the *Privacy Act*, including where there may be meaningful opportunities for individuals to make informed decisions and provide valid consent in a public sector context, as well as how individuals could be best supported to exercise control and consent in relation to their personal information under the *Privacy Act's* lawful authority-based governance model. These questions are fundamental given the federal government's publicly stated goal of moving towards a "tell us once" service delivery model, where data entered in one government system can be reused by multiple other government systems.

2) Require a necessity and proportionality standard for collecting personal information.

As noted above, the current *Privacy Act* does not require consent for the collection of personal information and instead, a government institution can collect information as long as it relates directly to an operating program or activity. Our experience has shown that this collection authority can sometimes be applied in an overly broad fashion. We have reported to Parliament that the shift towards digitization has made the collection, use, disclosure and retention of information much easier for government. Imposing a stricter threshold for collection under the *Privacy Act* would limit the over-collection of personal information by government.

This trend of over-collection in particular was once again made apparent in our investigation of complaints relating to Statistics Canada's collection of personal information about a large number of Canadians from a credit bureau and planned collection from financial institutions. To address this problem, our Office has recommended that the collection of personal information by federal institutions be governed by a necessity and proportionality standard.

Introducing a necessity and proportionality test into the law would effectively limit the risk of over-collection of personal information at the federal level because government initiatives would be carefully evaluated for privacy risks at the outset. The principle of necessity is already found in provincial and territorial legislation protecting personal information in the public sector, and is a commonly accepted standard to ensure that public bodies do not over-collect personal information. In order to demonstrate necessity, federal institutions would be required to define a pressing and substantial public objective.

Proportionality derives not from administrative law, but from human rights law where it is a well-known concept for balancing infringements of rights against the protection of other rights or important interests. The proportionality concept is also found in the GDPR under recital 4, and aspects of the concept have been interpreted by the Federal Court of Appeal to form part of PIPEDA, notably section 5(3). Adding an explicit proportionality requirement into the *Privacy Act* would place further limits on the government's collection of personal information to ensure an enhanced level of privacy protection.

3) Require organizations and federal government institutions to demonstrate their accountability.

Accountability is a key principle under PIPEDA and relates to an organization's duty over personal information protection as mandated under the law. While we see it as an important principle of

the law, we are increasingly noticing the ways in which it has become deficient in today's world of complex data flows and less than transparent business models. Our recent investigations into Facebook and Equifax, for example, revealed that accountability as traditionally framed in the law is not strong enough to protect Canadians from the intrusive practices of companies who say they are accountable, but are in fact found not to be.

The deficiencies in the *Privacy Act* are readily evident when compared to the more comprehensive set of fair information principles embodied in PIPEDA. The Department of Justice is currently examining what greater accountability would look like in a renewed *Privacy Act*. In its public statement on modernizing Canada's federal public sector privacy law, the Department of Justice has noted, for example, that a modernized *Privacy Act* should "demonstrate meaningful and transparent accountability, including effective oversight."

In short, the current accountability framework needs to become more robust.

Drawing from the lessons of recent investigations, we are advocating for an enhanced and strengthened law that will require demonstrable accountability. The law must not merely impose accountability obligations as under PIPEDA, for example, and then let organizations decide how they will comply – this is another form of self-regulation, which has proven to be untenable. More specifically, the following enhancements to the law would help to support demonstrable accountability:

- **Proactive inspection powers without grounds:** In today's world, where business and government service delivery models are opaque and information flows are increasingly complex, individuals are unlikely to file a complaint when they are unaware of a practice that might cause them harm. This is why it is so important for the privacy regulator to have the legal authority to proactively inspect the practices of organizations. The Privacy Commissioner has the authority under section 37 of the *Privacy Act* to carry out investigations at his discretion in order to ensure a government institution is compliant with specific sections of the Act. The addition of a similar provision in PIPEDA would move us towards a model of assured accountability and away from the current failed model of self-regulation in the private sector. These powers also currently exist in the UK and several other countries and are an essential mechanism for effective enforcement.
- **A requirement to provide evidence of accountability on demand:** Organizations and federal institutions should be required by law to maintain records to provide evidence of adherence with accountability requirements. The ability for an organization and federal institution to demonstrate true accountability becomes even more important in cases where consent is not practical or required, and organizations and federal institutions are expected to fill the protective void through accountability. This record keeping requirement would be necessary to facilitate the OPC's ability to conduct proactive inspections under PIPEDA, as outlined above, and is a deficiency that has been noted in our compliance work under the *Privacy Act*.

  Demonstrable accountability is also part of the solution in protecting Canadians in the context of transborder data flows. Our Equifax investigation has demonstrated that PIPEDA's accountability principle as currently framed is not always effective in protecting Canadians in a transborder context. To rectify this, the law must include at least a more robust accountability regime, through the adoption of demonstrable accountability, and possibly other supplemental measures, such as the European regime of standard contractual clauses. We note that elsewhere creative proposals are surfacing that seek to improve consumer privacy protections by

strengthening the obligations a business has towards its consumers. For example, New York's proposed privacy bill has introduced the concept of a data fiduciary, meaning businesses would have the responsibility to protect the personal information of their customers and would be sanctioned if they acted in a way that did not protect the interests of individuals.

- **A requirement to design for privacy and assess privacy risks at the start of the planning process:** Accountability involves building privacy assurance into the very design of a product, service or initiative, from the early phase of conception through to its execution, deployment and beyond. Privacy by Design (PbD), a concept developed by former Ontario Information and Privacy Commissioner Ann Cavoukian, is useful in this regard. In addition to an explicit design for privacy requirement, we view PIAs as an effective tool to assist with this effort, and have advocated on various occasions that they be mandatory in law. We note that various European jurisdictions have mandated data protection by design and by default measures, and have ensured its implementation through oversight from a data protection authority and/or requirement to conduct Data Protection Impact Assessments (similar to the PIAs currently used in Canada). Numerous non-EU jurisdictions have also created a legal requirement to implement data protection by design and default measures.

Moving towards stronger accountability requirements for organizations and federal government institutions is necessary to help achieve truly meaningful privacy protection in a digital age. Given the increased sharing of personal information that is occurring as part of product and service delivery, including across national boundaries, the accountability requirements for organizations and federal government institutions need to keep pace. We believe that in strengthening accountability, the interests of small and medium-sized enterprises (SMEs) must be taken into account. While all principles of a new privacy law should apply to all organizations, regardless of size, the manner in which principles are implemented may vary for SMEs. For instance, the recordkeeping obligations of SMEs under the accountability principle could be made lighter, unless they are engaged in activities that carry significant privacy risks for individuals.

4) Empower a public authority to issue binding guidance to ensure a practical understanding of what the law requires and to provide certainty to individuals, organizations and federal government institutions.

PIPEDA is a principles-based law written at a high level of generality, which has its advantages in a fast-evolving area like technology as it allows for application to circumstances that were potentially unforeseen at the time of drafting. However, a drawback of this approach is that such laws, when left at a level of abstraction, can be difficult to apply in practice with great certainty. Other mechanisms should exist to take general principles to a more concrete level. Effective instruments for assisting with interpreting the law can take the form of mandatory guidance, regulations and binding orders, to name but a few examples.

One model would be for a public authority to be given the power to issue binding subsidiary guidance under PIPEDA that would help to clarify how general principles of the Act are to apply in practice. The public authority could be either our Office, a government department or some other state entity. Binding guidance would ensure a more practical understanding of what the law requires, and could be amended more easily than legislation as technology and practices evolve. Another model

would be to rely on our Office's order-making authority to develop binding guidance through a succession of individual orders.

ISED has proposed that the development of codes of practice, accreditation/certification schemes and standards be encouraged in a reformed private sector law as a means of demonstrating due diligence in regards to compliance with certain provisions of the Act. They note that there is a need to recognize the value and utility of standards, codes and certification as tools to underpin privacy "rules" and suggest that adherence to codes and standards could incentivize compliance and potentially help enable a more proactive enforcement model. While we are open to such a scheme in principle, we strongly believe that if such instruments are meant to be legally binding, then the authority for their development and approval should be an emanation of the state that is independent from industry, and that businesses not be left to define their own rules. This would only serve to perpetuate the current self-regulation model. Any non-binding schemes for incentivizing adherence with the law would be welcome, but they should not be confused for law.

5) Permit the OPC to choose which complaints to investigate and, at same time, ensure individuals are given a private right of action.

Currently, the Commissioner does not have the power or authority to refuse or discontinue complaints under the *Privacy Act*, though he does under PIPEDA in certain defined circumstances. We have recommended to Parliament that the law should provide our Office with the ability to choose which complaints to investigate, in order to focus our limited resources on issues that pose the highest risk or may have the greatest impact for Canadians. At the same time, to ensure no one is left without a remedy, a modernized law must also give individuals a private right of action for violations to ensure they can pursue recourse.

Our Office, like many of our privacy and data protection counterparts, upholds several mandates with finite resources. Where our Office does not proceed with an investigation of a complaint, individuals should have the right to seek judicial redress on their own accord. This would help ensure that individuals' rights are respected and they are not left without a remedy. This right exists in the GDPR and is being considered elsewhere. For example, the *New York privacy act* that was before the State Senate Consumer Protection Committee at the time of drafting this report seeks to provide individuals with the right, among others, to sue companies directly over privacy violations.

6) Authorize regulators with different mandates to share information.

Meaningful protection of consumers and citizens in the fast-paced digital and data-driven economy understandably must involve several regulators, and they must be able to coordinate and share their work. A modernized law must allow different regulators to share information in certain circumstances in order to better coordinate their work. This change is needed because there are times when regulatory mandates overlap in the course of an investigation but regulators are not permitted to share relevant information. This does a disservice to Canadians, resulting in inefficiencies that can potentially delay recourse for individuals. Such a change could help to ensure the most effective remedy possible is available to Canadians, relying on the different expertise of various regulators. It could also allow our Office to provide various other regulators who do not have privacy expertise with information on how privacy implications factor into their decisions. Privacy is an increasingly cross-cutting issue given the widespread use of personal information across sectors.

7) Extend coverage of the law to all of federal government and political parties.

Currently the *Privacy Act* applies exclusively to those government institutions listed in Schedule 1 of the Act or those added in the definitions section (e.g., Crown corporations). We recommend that the Act be amended to extend its application to all federal government institutions, as well as Ministers' offices and the Prime Minister's Office. As the current Act does not apply to all of government, we have experienced barriers in completing investigative work where the scope of a complaint extended beyond listed entities. Expanding coverage of the law would allow our Office to exercise more effective oversight and ensure a common set of rules apply to the whole of government.

As well, it is imperative for privacy laws to explicitly extend to Canadian political parties. We have learned in recent times from the Facebook / Cambridge Analytica scandal that political parties are gathering significant amounts of personal information on voters as they adopt micro-targeting techniques. Such actions demonstrate the inextricable link between privacy and democracy. Specifically, it reveals how personal information about us can be used to sway our thoughts and actions, and in turn, undermine our democratic processes. While we have recently issued *Guidance for federal political parties on protecting personal information*, this is non-binding. The need to strengthen privacy protections and subject political parties to the rule of law is sorely needed.

8) Include additional protections against harms that result from infringements of human rights in a digital era.

Big data, artificial intelligence, automated decision-making and data profiling have made it imperative that individuals be afforded more privacy protection that ensures their fundamental human rights are respected in the digital era. We note that jurisdictions elsewhere have taken action to ensure there is a place in the law for rights specific to our new digital reality, including the right to be forgotten, data portability, and algorithmic transparency or explanation. These enhanced rights protecting privacy must, of course, be reconciled with other constitutional rights. For example, the right to be forgotten must be considered along with the right to freedom of expression.

In our Draft Position on Online Reputation, our Office set out its preliminary views with respect to matters related to online reputation, including the right to be forgotten. Our draft position, which was informed by both existing protections and gaps in federal private sector privacy law, included measures that call for the right to ask search engines to de-index web pages that contain inaccurate, incomplete or outdated information; removal or amendment of information at the source; and education to help develop responsible, informed online citizens.

Our Office has also brought a reference to the Federal Court to seek clarity on whether PIPEDA applies to Google's search engine service, which is an issue that arose in the context of a complaint to our Office against Google requesting that certain web pages be de-indexed from results for searches of the complainant's name. Though this preliminary jurisdictional issue is currently before the courts, we believe that it is incumbent on Parliament to consider the right to be forgotten and other proposed remedies for protecting online reputation, and that it would be inappropriate to wait to act on such fundamental issues.

Further reading

Guidelines for obtaining meaningful consent

"Report on Consent", Annual Report to Parliament 2016-2017

New York State Senate Bill S5642, *New York privacy act*

"Declined to investigate" and "discontinued" complaint dispositions under PIPEDA

Guidance for federal political parties on protecting personal information

Draft OPC Position on Online Reputation

Ultimately, we recommend that reformed legislation must incorporate rights that protect against harms that are unique to the digital era, including but not limited to ubiquitous surveillance, discrimination in profiling, automated decision-making, and behavioural data analytics. We are confident that industry and the government will be able to continue to develop useful services for Canadians and benefit in a world where the law recognizes and protects the full rights of Canadians.

Conclusion

Our laws have simply not kept pace with the reality in which they operate. Our reality is now one in which new business models that rely on personal information emerge daily, and the stockpiling of personal information is increasingly seen as a competitive advantage. It is a reality in which individuals, businesses and government are all seeking to harness the benefits of technology, often without a full understanding of the risks it poses. This increased reliance on technology, combined with the ease with which information flows across borders and changes hands makes it difficult for individuals to know if they are dealing with a human or a robot, an entity in Canada or elsewhere, or the public or private sector.

In this complex digital environment, what is clear is that our privacy laws need to be reflective of the current times, and more forcefully assert protections for the rights of Canadians. Now is the time for action.

Supplement to "Privacy Law Reform"

What follows are model preambles and purpose statements suggested as means to entrench privacy in its proper human rights framework.

These would serve to provide guidance as to the values, principles and objectives that should shape the interpretation and application of PIPEDA and the *Privacy Act*.

We recommend that both a preamble and a purpose statement appear at the opening of each of the two laws.

Proposed wording for PIPEDA

Preamble

WHEREAS privacy is a basic human right of every individual and a fundamental value reflected in international human rights instruments to which Canada is a signatory;

WHEREAS the right to privacy protects individual autonomy and dignity, and is linked to the protection of reputation and freedom of thought and expression;

WHEREAS privacy is essential to relations of mutual trust and confidence that are fundamental to the Canadian social fabric;

WHEREAS privacy is essential to the preservation of democracy and the full and meaningful enjoyment and exercise of many of the rights and freedoms guaranteed by the *Canadian Charter of Rights and Freedoms*;

WHEREAS the current and evolving technological context facilitates the collection of massive quantities of personal data as well as the use of these data, whether in identifiable, aggregate or anonymized forms, in ways that can adversely impact individuals, groups and communities;

WHEREAS the processing of personal data should be designed to serve humankind;

WHEREAS responsible processing of personal data can serve public interests such as economic growth, advances in health care and the protection of the environment;

WHEREAS this law protects the privacy rights of individuals while recognizing the legitimate interest of organizations to collect, use and disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances and in ways that do not represent surveillance;

WHEREAS the right to privacy must be balanced with other fundamental rights such as the right to freedom of expression in circumstances in which the collection, use or disclosure of personal information serves a legitimate public interest;

AND WHEREAS this statute has been recognized by the courts as being quasi-constitutional in nature;

Purpose

The purposes of this Act are:

(a) to implement the fundamental right to privacy of all persons in the commercial context through robust data protection that ensures that the processing of data is lawful, fair, proportional, transparent and accountable, and respects the fundamental rights and freedoms of individuals;

(b) to balance privacy rights with the right to freedom of expression in circumstances in which the collection, use or disclosure of personal information serves a legitimate public interest;

(c) to balance privacy rights, where appropriate, with what the public interest requires;

(d) to protect the privacy rights of individuals while recognizing the legitimate interest of organizations to collect, use and disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances and in ways that do not represent surveillance;

(e) to provide individuals with quick and effective remedies when their privacy rights have not been respected and to ensure the ongoing compliance by organizations with their obligations under this Act.

Proposed wording for the *Privacy Act*

Preamble

WHEREAS privacy is a basic human right of every individual and a fundamental value reflected in international human rights instruments to which Canada is a signatory;

WHEREAS the right to privacy protects individual autonomy and dignity, and is linked to the protection of reputation and freedom of thought and expression;

WHEREAS privacy is essential to the relations of mutual trust and confidence that are fundamental to the Canadian social fabric;

WHEREAS privacy is essential to the preservation of democracy and the full and meaningful enjoyment and exercise of many of the rights and freedoms guaranteed by the *Canadian Charter of Rights and Freedoms*;

WHEREAS the current and evolving technological context facilitates the collection of massive quantities of personal data as well as the use of these data, whether in identifiable, aggregate or anonymized forms, in ways that can adversely impact individuals, groups and communities;

WHEREAS all individuals have a constitutional right to be free from unreasonable search or seizure, including the right to be free from unwarranted state surveillance;

WHEREAS the federal government must only collect, use or disclose personal information in ways that are lawful, fair, proportional, transparent and accountable and only to serve individual Canadians or the legitimate public interest;

WHEREAS this statute has been recognized by the courts as being quasi-constitutional in nature;

Purpose

The purposes of this Act are:

(a) to implement the fundamental right to privacy of all persons with respect to their personal information in the federal public sector through robust data protection that ensures that the processing of personal information is lawful, fair, proportional, transparent and accountable, and respects the fundamental rights and freedoms of individuals;

(b) to balance the privacy rights of individuals with the government's requirement to collect, use and disclose personal information for purposes that demonstrably serve the public interest;

(c) to provide individuals with quick and effective remedies when their privacy rights have not been respected and to ensure the ongoing compliance by institutions with their obligations under this Act.

Parliamentary activities

While the value of privacy remains timeless, Canadians' concern about privacy risks has increased since the inception of our Office in 1983. In less than a generation, dramatic advances in information technology have transformed how companies interact with consumers, and how governments interact with citizens. Along with the great benefits of the digital economy and digital government come the great risks that materialize in massive data breaches and pervasive surveillance.

Reflecting this societal shift, parliamentarians have been calling more and more often on our expertise to help them examine legislation that will have a meaningful impact on Canadians' rights. In fact, we appeared before Parliament more often in calendar year 2018 than in any other in the Office's 35 years of existence.

Below is a summary of some of the advice provided by our Office to Parliament in 2018-2019 in the context of various committee studies.

Legislation

Bill C-76, *Elections Modernization Act*

Against the backdrop of controversies around the world regarding foreign interference in the democratic process, Bill C-76, the *Elections Modernization Act*, introduced changes to federal electoral processes and procedures.

Unfortunately, the Act did not make federal political parties subject to privacy laws. The legislation created a new requirement for federal political parties to develop written privacy policies, something most of the national parties had already done. These policies must have prescribed content, but there is no requirement that the substance comply with international privacy standards.

We advocated for federal political parties to be made subject to internationally recognized privacy principles and that an independent third party have the authority to verify compliance. These recommendations were not adopted.

Parties are left to define the standards they want to apply. Ultimately, the *Elections Modernization Act* adds nothing in terms of privacy protection.

It is worth noting that many jurisdictions around the world have privacy laws that govern political parties, including the EU, the UK, New Zealand, Argentina and Hong Kong. It is also useful to recall, when we asked Canadians a decade ago, 92% of those surveyed believed political parties should be subject to some form of privacy law.

In April 2019, our Office, along with the Chief Electoral Officer, issued joint guidance for federal political parties on protecting personal information. The guidance was developed to help political parties comply with their new legal obligations relating to privacy policies, but it also outlines a number of privacy best practices, which parties are encouraged to follow in order to protect personal information and help engender trust among Canadians.

Further reading

Bill C-76, *Elections Modernization Act*

Opening Statement by Daniel Therrien, Appearance before the Standing Committee on Procedure and House Affairs on the study about Bill C-76, *Elections Modernization Act*

2009 Survey of Canadians, figure 5.10: Agreement that Political Parties Should be Subject to Privacy Legislation

Guidance for federal political parties on protecting personal information

Bill C-74, *Budget Implementation Act*

The Commissioner appeared before the Standing Senate Committee on Banking, Trade and Commerce examining Bill C-74, the *Budget Implementation Act, 2018, No. 1*. The Bill included amendments aimed at removing barriers to collaboration among federally regulated financial institutions and financial technology organizations, or "fintechs."

The Commissioner noted that the government's efforts appeared to have been directed towards innovation without ensuring that privacy is adequately considered. For example, it was unclear whether consent would be obtained as per our Guidelines for Obtaining Meaningful Consent. In addition, the Commissioner underlined that he does not have the authority to require organizations to apply reasonable measures when it comes to consent.

In a follow-up letter to the Committee, the Commissioner proposed enhancing the provisions in PIPEDA that deal with the obligation to obtain meaningful consent and introducing new provisions that enable our Office to issue binding orders to organizations that fail to comply with PIPEDA's requirements.

The Committee's subsequent report on Bill C-74 stated the issue of legislative reform warranted further study by the federal government. Committee members stated that while PIPEDA was outside the scope of their study, Canada's privacy laws did need to be updated and "made consistent with global standards."

Since that appearance, our Office has had follow-up conversations with Finance Canada on their proposed next steps, and we look forward to further discussions.

Further reading

Bill C-74, *Budget Implementation Act, 2018, No. 1*

Opening statement by Daniel Therrien, Appearance before the Standing Senate Committee on Banking, Trade and Commerce on Division 16 of Part 6 of Bill C-74

Guidelines for Obtaining Meaningful Consent

Follow-up letter to the Standing Senate Committee on Banking, Trade and Commerce on Bill C-74, *Budget Implementation Act, 2018, No. 1*

Report of the Standing Senate Committee on Banking, Trade and Commerce on the subject matter of Bill C-74

C-59, *An Act respecting national security matters*

Last year's annual report noted that our Office had appeared before the House of Commons Standing Committee on Public Safety and National Security on Bill C-59 and sent follow-up submissions to the Committee. In April 2019, the Commissioner appeared before the Senate Standing Committee on National Security and Defence during its study of the amended version of the Bill.

The Commissioner was generally pleased to see that while the amendments adopted in the Commons were slightly different than those he has proposed, they nonetheless achieved the same goal of providing a sensible necessity test for information sharing between national security agencies.

As for sharing confidential information between oversight bodies, the amended Bill provides our Office with the authority to share information and coordinate activities with the National Security and Intelligence Review Agency, but not with the National Security and Intelligence Committee of Parliamentarians.

While imperfect, the Bill as ultimately adopted by Parliament remains fairly balanced and a clear improvement over previous law.

Further reading

Bill C-59, An Act respecting national security matters

Opening statement by Daniel Therrien, Appearance before the Standing Committee on Public Safety and National Security on Bill C-59, *An Act respecting national security matters*

Opening statement by Daniel Therrien, Appearance before the Senate Standing Committee on National Security and Defence on C-59, *An Act respecting national security matters*

Parliamentary studies

In addition to legislation, parliamentary committees conducted studies on a variety of issues with privacy impacts, including the following.

Digital Government Services

The Commissioner and other senior representative from our Office appeared before ETHI related to its study of the privacy implications and potential legal barriers stemming from the implementation of digital government services at the federal level. This study produced recommendations on how the government could improve its services while also protecting Canadians' privacy and security.

Our remarks referenced the Government's November 2018 Data Strategy Roadmap, which proposes changes to how the federal public service collects, manages and governs data. We cautioned that what's viewed as a legal barrier to some may be considered a privacy safeguard by others. We urged the Committee to remember that, while adjustments may be desirable, any new legislation designed to facilitate digital government services must respect privacy as a fundamental human right.

We also commented on the Estonian model, which is often highlighted for its technological architecture. We noted that elimination of silos within the Estonian government's information holdings did not lead to borderless horizontal management of personal data across government. Rather, information sharing appears to be based on legislation that sets conditions generally consistent with internationally recognized Fair Information Practice Principles and with the EU's GDPR.

The Estonian model also provides a strong role for Estonia's data protection authority as well as powers to issue binding orders, apply for commencement of criminal proceedings and impose fines when data is processed in

an unlawful manner, or for violations of the requirements for managing or securing data. We recommended that our Office should have a similar strong, proactive oversight role, consistent with our advice on *Privacy Act* reform. The best way for Canada to position itself as a digital innovation leader is to demonstrate how we can establish a framework for innovation that also successfully protects Canadian values and rights and our democracy.

Further reading

Opening statement by Daniel Therrien, Appearance before ETHI on Privacy of Digital Government Services

Privy Council Office, A Data Strategy Roadmap for the Federal Public Service

International Grand Committee on Big Data, Privacy and Democracy

Legislatures in many countries around the globe are grappling with the impacts of the complex digital environment on democratic processes and institutions. In May 2019, Canada hosted an International Grand Committee of Parliamentarians seeking solutions to these challenges in the aftermath of investigations into Facebook and Cambridge Analytica and their troubling revelations.

The Committee, made up of representatives from 11 countries, declared that social media platforms should strengthen privacy rights and data protections and that regulation may be necessary to achieve this. In particular, to prevent digital activities that threaten social peace and interfere in open and democratic processes.

Witnesses appearing before the Committee discussed issues related to big data, privacy and democracy. The three days of testimony provided great insight into larger issues such as surveillance capitalism, the power of technology and data, disinformation, algorithmic transparency, the attention economy, and online hate speech. Committee members were also briefed on practical matters such as how large platforms operate, changes in the use of the Internet, and the role of third parties and intermediaries in the collection and use of personal data.

Commissioner Therrien was among the experts whose testimony the members of the Grand Committee sought out. The Commissioner urged states and international representatives to think beyond just questions of privacy and data protection, as vitally important as they are. We cautioned that democratic institutions and citizens' faith in the electoral process are now under a cloud of suspicion and distrust. He highlighted that the digital tools that could engage a new generation of citizens in the electoral process are increasingly also being used to subvert, not strengthen, democracies.

Along with other witnesses, he argued that modernized regulatory approaches, stronger laws and demonstrable accountability are critically important to restore citizen trust.

Further reading

Opening statement by Daniel Therrien, International Grand Committee on Big Data, Privacy and Democracy

Open banking

Representatives from our Office appeared twice before the Standing Senate Committee on Banking, Trade and Commerce on its open banking study and our Office made a submission to Finance Canada as part of its consultations on open banking.

Open banking enables consumers and businesses to share financial information with a wider range of service providers in exchange for financial services.

Our Office stressed the need to promote trust and confidence in the digital economy, and to ensure that individuals are not viewed as a commodity. Commissioner Therrien underscored that privacy is not a right we simply trade away for innovation, efficiency or commercial gain.

Specifically, we called for consistent ground rules for open banking, and we recommended the development of standards, including technical and privacy standards. We also noted that our Office would be pleased to provide privacy expertise to support the development of Canadian standards. In addition, we voiced support for accreditation and authorization for new players to participate in an open banking initiative.

We also recommended that any policy or legislative framework developed to support open banking explicitly refer to the existing privacy legislative framework in Canada and that oversight in this realm be exercised by our Office.

In addition to those points, our Office noted that it is essential for businesses operating in the digital economy to follow our Guidelines for Obtaining Meaningful Consent.

We expressed our willingness to support and work with the government to address our recommendations, and assist with future discussions related to the planning, implementation and oversight of open banking – including the development of the standards required to facilitate information sharing.

Further reading

Opening statement by Gregory Smolynec, Appearance before the Standing Senate Committee on Banking, Trade and Commerce on open banking, February 2019

Opening statement by Gregory Smolynec, Appearance before the Standing Senate Committee on Banking, Trade and Commerce on open banking, May 2019

A Review into the Merits of Open Banking: Submission to the Department of Finance Canada

Guidelines for Obtaining Meaningful Consent

The *Privacy Act*

A year in review

The following section highlights some of our key initiatives under the *Privacy Act*.

The *Privacy Act*'s advanced age was readily apparent in some of our investigations. We saw how the Act is not up to the task of confronting the challenges of the digital age.

When the Act came into force more than three decades ago, many of the issues examined in this year's *Privacy Act* investigations – such as border officers examining mobile devices and government departments acquiring personal information from corporate data brokers – were still in the realm of science fiction.

In particular, our investigation into to mass data collection initiatives at Statistics Canada illustrated the pressing need for the *Privacy Act* to include a requirement for government institutions to demonstrate the necessity for collecting personal information before doing so.

Some of the complaints we investigated touch on long-standing privacy issues such as citizens' access to the information government holds about them, and public servants' right to privacy in the workplace.

We continued to note inconsistencies in public sector breach reporting, and saw signs of systemic under-reporting, bolstering our calls for mandatory breach reporting in the public sector through a reform of the *Privacy Act* rather than through a Treasury Board directive.

Outside the context of formal investigations, we urged federal government institutions to prioritize timely responses to Canadians' access requests. We increased our efforts to engage proactively with public servants to help them improve their privacy practices. Amongst new pressures to adopt digital services and technologies, we provided advice to the federal public sector in relation to various specific programs and initiatives.

Operational updates and trends

In 2018-2019, our Office accepted 1,420 complaints under the *Privacy Act,* up from 1,254 a year earlier.

Despite this increase over the previous reporting period, we were able to prevent further growth of the backlog of *Privacy Act* complaints and reduce our average treatment times for complaints closed through early resolution by close to one month.

The progress we have made in these areas can be attributed in part to the creation of the Compliance, Intake, and Resolution Directorate. This Directorate receives and addresses complaints at the front-end, acting as a filter to help ensure that complaints sent to formal investigation merit a thorough assessment.

The Directorate does this, for example, by overseeing the early resolution of complaints, an efficient mechanism that results in a satisfactory outcome for all parties. For individuals, it means having their concerns addressed quickly. Respondent institutions benefit by avoiding a lengthy and resource-consuming more formal investigation process.

Early resolution has consistently been used to address a third of *Privacy Act* complaints. Of the 1,366 *Privacy Act* complaints we closed in 2018-2019, 433 were handled through early resolution.

We have also worked to become more effective after investigations have been completed. We expanded the functions of our Compliance Monitoring Unit to include *Privacy Act* investigations in addition to those under PIPEDA. The unit oversees the implementation of recommendations made during investigations to assess whether federal institutions meet their commitments to Canadians under federal privacy law. We expect this step will result in more consistent implementation of privacy-sensitive practices across the public sector.

We anticipate that temporary funding announced in the 2019 federal budget will increase our capacity to reduce the backlog of complaints.

Prioritizing timely responses to Canadians' access requests

Despite our best efforts to work with federal institutions to prevent or mitigate Canadians' privacy concerns, there remain instances where federal departments fail to promptly address complaints concerning delayed responses to access requests made under the *Privacy Act*.

In the past, we generally did not close our investigations into these complaints until the complainant received their requested information. This often resulted in unreasonably lengthy delays, sometimes causing the investigation to stretch well over a year.

Going forward, our Office will seek to better empower complainants who raise issues of institutions failing to respect legislated time limits. In instances where repeated unsuccessful attempts by our Office to have an institution provide the complainant with a timely response to their access request under the *Privacy Act*, we will deem the institution's nonresponse a refusal of access. The next step is the issuance of a final report detailing this, which the complainant may then take to Federal Court.

This past year, we issued 31 deemed refusals against three government institutions: Health Canada, the Royal Canadian Mounted Police (RCMP) and Correctional Services Canada (CSC).

Our preference remains to work collaboratively with institutions where there is good faith, cooperation and progress. However, where there are unreasonable delays, our priority is to ensure Canadians are empowered to exercise their privacy rights.

Our Office also held a workshop in the spring of 2019 for privacy and program staff across a range of federal departments and agencies on informal disclosures. The event allowed our Office and participants to explore challenges and innovative approaches to informally disclose personal information in response to requests received for this information by individuals. We were encouraged by the level of engagement.

Participants were able to identify challenges related to informal disclosures, including:

- difficulties related to decentralizing the processing of informal requests within institutions;
- inconsistent training, knowledge, and views of program staff compared to access to information and privacy (ATIP) office staff;
- many requesters prefer to follow formal channels to request their personal information; and
- the potential for severe consequences should a privacy breach occur as part of the processing of informal requests.

The workshop provided an opportunity to explore solutions to many of these issues. For example, one of the ideas discussed was to create or assign a dedicated team within the ATIP office to process informal requests. Defined processes and mechanisms for common or frequent requests could support staff. At the same time, clearer information on websites could better inform individuals about where and how to start searching for their personal information.

Other suggestions included using triage mechanisms to prioritize and organize requests; using new technologies to assist in processing informal requests; and changing business processes to include proactive sharing of information.

We have included links to the full reports of findings or case summaries for some of the investigations summarized in these pages. These reports of findings and case summaries are considered to form an integral part of this annual report and are being submitted to Parliament alongside it.

Statistics Canada: Invasive data initiatives should be redesigned with privacy in mind

Issues highlight the need for necessity and proportionality to be required as a matter of law

In the late fall of 2018, media reports highlighted that Statistics Canada had collected detailed credit information, and was proposing to collect detailed financial information, about millions of Canadians from private sector companies – without individuals' prior knowledge or consent.

The stories prompted a storm of outrage. Our Office received more than 100 complaints related to this collection of individuals' credit history and the proposed collection of individuals' financial transaction and account balance information from banks.

Individuals told us they felt Statistics Canada was invading their right to privacy. Concerns were raised regarding: the Agency's legal authority to collect the information; transparency about the collections; the handling of collected information including potential intentional or unintentional disclosures; and individuals' right of access to the information collected.

Line-by-line financial transaction information can paint an intrusively detailed portrait of an individual's lifestyle, consumer choices and private interests, including lawful choices individuals would not want the government to know about. A complete record of financial information is therefore extremely sensitive personal information. Similarly, credit information tells a detailed story of an individual's current and historic debt levels and is sensitive by its very nature.

Canadians were justifiably concerned about the impact of these projects on their privacy rights.

Our investigation did not find that Statistics Canada had violated current laws, however, it did raise significant privacy concerns about the initiatives.

The matter also highlights the urgent need for legislative reform to ensure better privacy protection for Canadians in a digital era that has enabled federal institutions to collect, analyze and store vast amounts of personal information.

About the projects

Our Office opened an investigation in October 2018. At issue were Statistics Canada's Credit Information Project and Financial Transactions Project.

The two programs are part of a modernization initiative by Statistics Canada, which aims to use new public and private sources of administrative data.

The Agency noted that statistical organizations around the world are experiencing decreasing survey response rates and increasing costs, while facing growing demands from governments and the private sector for more timely and detailed statistical information about the population.

Through the Credit Information Project, Statistics Canada collected data from credit reporting agency TransUnion, which transferred to Statistics Canada historical credit data going back to 2002, as well as personal identifiers such as name, date of birth, social insurance number, and address. In all, TransUnion transferred approximately 44 million records comprising the information of about some 24 million individuals to Statistics Canada. It was explained that the discrepancy in these figures was in part attributed to duplicate records for individuals and records for deceased individuals.

We found that Statistics Canada is able to link this data to other information related to individuals contained in its data holdings, such as household income and property information collected from other sources. Although Statistics Canada replaces direct identifiers with an artificial number that is maintained on a linkage key, to which a small and limited number of Statistics Canada employees have access, the information remains identifiable through the linkage key and can be the subject of future linkages by Statistics Canada.

The Financial Transactions Project, meanwhile, aimed to measure household expenditures by collecting the detailed financial transaction and account balance information of 500,000 individuals per year directly from financial institutions.

The project, which did not reach the implementation stage, was proposing to collect the date and value of all transactions recorded for each of the individuals in their personal accounts, a description of each transaction, the payee's name in the case of payments, and the ending balance of the account after the transaction was completed. The project would have also collected the account holders' personal identifiers, including name, social insurance number, date of birth, phone number and home address.

Our findings

Given no personal information was actually collected as part of the Financial Transactions Project, we did not issue a finding in that matter.

However, we had serious concerns that, as originally designed, the project would have exceeded Statistics Canada's legal authority to collect personal information. Critically, Statistics Canada's request would have required the creation of new records not already maintained by financial institutions. In addition, according to the institutions, this would increase sector security risks in that the compilation of this sensitive information would have created an attractive, high-value target for hackers.

In the case of the Credit Information Project, we ultimately determined that Statistics Canada had the legal authority to collect the information at issue as it involved the collection of records already maintained by TransUnion. We therefore concluded the complaints related to that Project were not well founded.

However, we identified significant privacy concerns with respect to both projects, even though we did not find contraventions of the current Act. This underscores certain shortcomings of the *Statistics Act* as well as the *Privacy Act*.

In particular, we found that while Statistics Canada gave several administrative and strategic reasons to justify the projects, the Agency did not demonstrate that, as designed, the projects were necessary or proportionate to the invasion of privacy they entailed.

We are pleased that Statistics Canada put both projects on hold in the fall of 2018 and, following discussions over the course of our investigation, has agreed to implement our recommendations in full, including ensuring that necessity and proportionality would be respected before moving forward with the projects in question.

Necessity and proportionality

Necessity and proportionality are key concepts in privacy protection. It is critical for federal institutions to demonstrate that privacy-invasive activities and programs are necessary to achieve a pressing and substantial purpose and that the intrusion is proportional to the benefit to be gained.

Although not a legal requirement in the current federal law, the Treasury Board of Canada Secretariat (TBS) Directive on Privacy Practices requires that federal institutions only collect personal information where it is "demonstrably necessary" for its operating programs or activities. It is not sufficient for federal institutions to rely on their general mandate to justify the necessity of privacy intrusions.

Our Office has been recommending for several years that the collection of personal information by federal institutions be governed by a necessity and proportionality standard under the law.

Many other jurisdictions both in Canada and abroad have already adopted a necessity standard as a legal requirement.

Canada should follow suit and update the *Privacy Act* to include this standard.

In practical terms, we have been encouraging federal institutions to assess the following questions for activities and programs that are particularly invasive:

- Is the measure demonstrably necessary to meet a specific need?
- Is it likely to be effective in meeting that need?
- Is the loss of privacy proportional to the need?
- Is there a less privacy invasive way of achieving the same end?

During our investigation, Statistics Canada described the public objective of the two projects in general terms and therefore failed to demonstrate necessity.

However, based on information the Agency provided, we have inferred that the objective of the Credit Information Project is to provide valid statistical information to support policies directed at addressing vulnerabilities in Canada relating to personal finances, especially household debt, interest rates, and developments in the housing market.

Meanwhile, we inferred the objective of the Financial Transactions Project is to fill data gaps in order to produce valid statistical information across household groups and to support specific economic and social policies, such as anti-poverty policies targeted at vulnerable populations, and policies to pre-emptively mitigate the effects of economic recessions.

We found that these objectives, if validated by Statistics Canada, could reasonably meet the requirement for a pressing and substantial public goal. That being said, we also found that further consideration would need to be given as to whether all of the personal information that Statistics Canada seeks to collect for the projects is demonstrably necessary and proportional to achieve its objectives. We concluded that, as originally designed, the projects raised serious concerns as to whether the degree of privacy loss was proportional to the needs.

Statistics Canada had initially argued that because its purposes are limited to producing aggregate statistics and that the Agency is required to keep personal information it collects confidential, the collections are "proportional".

We accepted that these are important factors in the proportionality analysis, but they are not sufficient. Otherwise, there would be seemingly no limit to what personal information Statistics Canada could collect pursuant to its mandate.

Transparency and security

The investigation also identified a few other concerns.

We found Statistics Canada had failed to be adequately transparent with respect to the collection of personal information as contemplated under the projects.

As well, although Statistics Canada has taken significant steps to isolate and minimize access to data and protect against external threat actors, it could improve its security safeguards to mitigate against internal threat vulnerabilities via monitoring for internal unauthorized access and use.

Recommendations

We issued several recommendations, which Statistics Canada has committed to implement.

Specifically, we recommended that Statistics Canada:

- not continue to proceed with the Credit Information Project as originally designed; we also strongly encouraged Statistics Canada to dispose, in due course, of the personal information already collected that would not have been collected via the redesigned project;
- not proceed with the Financial Transactions Project as originally designed;
- work with our Office to redesign the Credit Information Project to respect the principles of necessity and proportionality;
- work with our Office to complete the redesign of the Financial Transactions Project to respect the Agency's lawful authority and the principles of necessity and proportionality before implementing the Project;
- increase transparency regarding prospective collections of personal information from administrative sources in order to maintain public trust; and
- implement measures to address risks posed by internal threat vulnerabilities.

Beyond the recommendations we have made to Statistics Canada, we are calling on Parliament to consider legislative reform of the *Statistics Act* and the *Privacy Act* to address the appropriate balance between the privacy of individuals and the public interest in obtaining personal information from administrative data sources, including private sector companies.

The provision in the *Statistics Act* that permits Statistics Canada to gain access to administrative records can be traced back to 1918, well before organizations began collecting and storing large amounts of personal information electronically.

Furthermore, the *Statistics Act* does not oblige Statistics Canada to demonstrate the necessity and proportionality of administrative data collection involving personal information, data minimization, transparency and retention, or regulate when the Agency can use the information to make linkages for other studies.

The deficiencies in the *Statistics Act* would not be as troubling if the *Privacy Act* were not so out of date. The *Privacy Act* should include a necessity and proportionality requirement for the collection of personal information by federal institutions.

Next steps

We welcome Statistics Canada's commitment and openness to changing their methods towards better integrating privacy protective measures, such as necessity and proportionality, into the development of new statistical initiatives. We believe it is an important step to enhancing public trust.

We hope Statistics Canada's experience can serve as an inspiration for other federal institutions as they continue to align their activities with the government's Data Strategy Roadmap for the Federal Public Service.

Report of findings

Investigation into Statistics Canada

Other key investigations

Investigation highlights serious flaws related to border searches of digital devices

Searches of personal digital devices – particularly cellphones, tablets and laptop computers – by Canadian border services officers prompted several complaints against the Canadian Border Services Agency (CBSA).

Digital devices can store vast amounts of an individual's most private and personal information. When connected online, they provide a gateway to personal information that extends far beyond what is traditionally carried in luggage. As a result, there are significant privacy interests at stake in the search of digital devices.

During our investigation of the complaints, we discovered that the content reviewed by the officers in these cases included, for example, documents, text messages, photographs, Facebook and WhatsApp messages, a history of websites visited, and online banking information.

The complainants, all Canadian citizens returning from travel abroad, questioned the CBSA's authority to conduct such searches.

The *Customs Act* allows border officers to examine any "goods" that have been "imported" into Canada for customs-related purposes to ensure compliance with the laws administered or enforced by the Agency. "Goods" are defined to include "any document in any form" and the CBSA took the position that this encompasses electronic documents contained on digital devices.

The Agency acknowledged that its authority does not extend to examining electronic documents that are not stored on a digital device, but that could be accessed from a device by connecting to the Internet.

To ensure officers access only information stored on a device, the CBSA has an internal policy requiring that Internet-enabled devices have their network connectivity disabled prior to a search.

The CBSA's policy also states that digital device searches should not be done as a matter of routine. It authorizes border officers to conduct progressive examinations of digital devices when there are a "multiplicity of indicators" of possible non-compliance with legislative requirements or further to the discovery of undeclared, prohibited, or falsely reported goods. The policy requires that the officers record the types of data examined and their reasons for doing so.

The investigation found multiple failures by CBSA officers to follow the CBSA's internal policy as well as requirements set out under the *Customs Act*.

For example, in one case, an officer used the complainant's device to access her online banking information, information that was not stored on the device and that was accessible only via the Internet.

Furthermore, the CBSA acknowledged that in four of the six cases, the device was not switched to airplane mode, contrary to agency policy. In the remaining two instances, the officers did not have notes indicating whether airplane mode was engaged.

We also found additional violations. In one of the cases, an officer took photographs of the content on a complainant's cellphone as evidence of a possible *Criminal Code* offence – inconsistent with the Agency's authority to copy records under the *Customs Act* and to seize evidence under the *Criminal Code*.

Furthermore, in all six cases examined, officers failed to record the indicators that led to the device searches, the areas of the devices accessed, or the reasons why those areas were searched.

The multiple failings we identified led us to conclude that there are insufficient training, awareness and accountability mechanisms to ensure that border officers are meeting the requirements set out in the *Customs Act,* the *Privacy Act* and under CBSA policy. As a result, Canadians' privacy rights are not being respected during device searches at border points.

The failings identified in the CBSA's practices point to chronic issues, which directly affect the CBSA's accountability to the public in both the exercise of the powers conferred upon it, as well as in meeting the requirements of the *Privacy Act.*

We made several recommendations to the CBSA to correct the deficiencies we observed. In particular, we recommended that the CBSA:

- Implement and document staff participation in a mandatory training program for all new and existing border officers and their supervisors to ensure officers are properly trained to conduct progressive examinations of digital devices and media.
- Establish oversight and review measures to monitor border officers' compliance with CBSA policy and practices with respect to the examination of digital devices, including officer inspections, notebook or system audits, and system flags for digital device examinations.
- Carry out an independent audit of the application of its policy and operational framework for the examination of digital devices under the *Customs Act.*
- Update its Customs Enforcement Manual to reflect the requirements of the CBSA's current policy.
- Make the policy, including any other relevant manuals, operational bulletins, etc., available on its website to provide greater transparency and accountability to the public.
- Compile and produce statistical data relating to its examination of digital devices and proactively make this information available to the public.

The CBSA accepted our Office's recommendations. Consequently, we consider all six complaints well founded and conditionally resolved.

In addition, our Office urges Parliament to amend the *Customs Act* to better protect the privacy of people crossing the border, and has written to both the Minister of Public Safety and Emergency Preparedness, and the Minister of Border Security and Organized Crime Reduction to that effect.

Specifically, we believe that the *Customs Act* should be updated to recognize that digital devices contain sensitive personal information and that these devices are therefore not mere "goods" within the meaning of the Act. As well, the Act should include a clear legal framework for the examination of digital devices and the threshold for examinations of digital devices should be elevated to "reasonable grounds to suspect" a legal contravention.

Report of findings

Investigation into CBSA

Global Affairs Canada seeks personal travel details from employee's diplomatic passport

A Global Affairs Canada (GAC) employee who had been issued a Government of Canada diplomatic passport and posted overseas had sometimes used his diplomatic passport for personal travel. As a result, his personal travel information (visas, border crossing stamps, dates of personal travel, etc.) was recorded in it.

GAC asked the employee to return the diplomatic passport as evidence in an administrative investigation. When he submitted photocopied pages of his passport demonstrating his work-related travel, the Department insisted he submit the original booklet. The complainant refused to do so, arguing that Global Affairs requires certain employees to use their diplomatic passports for personal travel.

GAC contended the diplomatic passport is property of the federal government and can be requested at any time and that, in this instance, it had authority to collect the complainant's personal travel information related to alleged misconduct. The Department did not provide any information regarding the nature of the administrative investigation.

A diplomatic passport contains the individual's name, date of birth and citizenship as well as personal travel history. The *Privacy Act* stipulates that "no personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution."

GAC failed to show how the complainant's personal travel was linked to, or the subject of, its investigation. Ultimately, no collection of the complainant's personal information occurred given that he did not return the diplomatic passport as requested. However, our Office concluded that the complaint was well founded.

Given the potential systemic nature of this issue and the possible impact on other individuals using diplomatic passports, we recommended GAC clarify the terms of its policy and practices related to the personal use of diplomatic passports and their privacy implications. We also recommended this information be communicated to people who may be affected by any personal use of a diplomatic passport. For example, GAC could advise diplomatic passport holders of the circumstances in which it may collect personal travel information at the same time it advises them of the permissible uses outlined in the Ministerial Instructions. GAC disagreed with our recommendations but nevertheless agreed to undertake a review of the information that is provided to users of diplomatic passports about the collection and use of their personal information.

Report of findings

Investigation into GAC

Inaccurate information leads to inadvertent hire, pay problems for public servant

A case of mistaken identity proved exasperating and costly for an employee of Public Services and Procurement Canada (PSPC) who was inadvertently hired for a position at ISED for which he had not even applied.

The mix-up related to a human resources software system – MyGCHR – that automates human resources functions such as staffing, classification, scheduling and leave. PSPC is responsible for implementing, hosting and maintaining MyGCHR and providing training to the federal institutions that use it.

When a department wants to hire someone, it checks to see if the individual has a profile on the MyGCHR system. If so, the person is then selected and the profile is sent to the hiring department.

At the time of the incident, ISED human resources officials had instructions to search MyGCHR using an individual's first and last name. They had not been instructed to consistently use a third data field, such as a Personal Record Identifier (PRI) or date of birth.

The problem in this case was that the complainant – who shared the same name as the successful candidate – was selected in the system even though he had not applied for the available position. Because of the mistake, the complainant was "terminated" from his position at PSPC within MyGCHR and missed some pay periods while the problem was sorted out.

The complainant alleged that ISED contravened the accuracy provisions of the *Privacy Act* when it used inaccurate information about him in staffing a position. In response to the error, ISED created a document advising employees that the identity of individuals must be validated using data such as a PRI or date of birth.

Since ISED is not responsible for making changes to MyGCHR, we are satisfied that it has taken reasonable steps to ensure the accuracy of information it uses when selecting profiles from this system. However, MyGCHR is used widely across government and still allows individuals to be selected using only first and last name, with no other data fields required.

Report of findings

Investigation into ISED

Canadian Transportation Agency denies access to airline passenger rights advocate's personal information

An air passenger rights advocate filed a complaint accusing the Canadian Transportation Agency (CTA) of unfairly invoking exemptions to disclosure in response to his request for access to his personal information.

The CTA had provided access to 33 full or partial pages of records but withheld 760 pages of records in their entirety, claiming this was consistent with provisions of the *Privacy Act*. In many cases, the information withheld contained views about the complainant's conduct or other information about the complainant. The other information included how the CTA handled his submissions and details the Agency had collected about the complainant from news articles. The information consisted largely of communications between CTA staff members, not notes taken by decision-makers that would be covered by adjudicative privilege.

However, the complainant was told most of his information did not conform to the legislation's definition of personal information since he was acting as a representative of a consumer rights advocacy group and not on his own behalf. The CTA argued that the complainant's name should not be considered his personal information where it relates to a regulatory or adjudicative matter that he brought to the attention of the CTA on behalf of an organization.

The complainant countered that the advocacy group he represents is not incorporated as a separate legal entity, and that all complaints filed with the CTA and any resulting legal action was undertaken under his own name.

Our Office found that the CTA relied on an incorrect interpretation of the definition of personal information in the Act to withhold information from the complainant and that his complaint was well founded. On this basis, we recommended that the CTA provide the complainant with access to his personal information

that had been withheld subject to the other applicable exemptions such as solicitor-client privilege.

The CTA was given until March 1, 2019, to provide a complete response to the complainant. Although it was not able to meet this deadline, the CTA notified our Office that it provided the complainant with the additional information on March 18, 2019. The complainant in this matter has filed an application to the Federal Court under section 41 of the Act with respect to the CTA's response to his request. At the time of writing this report, the matter was still before the Court.

Report of findings

Investigation into the CTA

Employment and Social Development Canada uses data broker list to send unsolicited emails

A complaint against Grey House Publishing Canada surrounding PIPEDA infractions also led to a *Privacy Act* complaint against Employment and Social Development Canada (ESDC). These complaints provide an interesting example of the intersection between the provisions of the *Privacy Act* and PIPEDA upon the collection and use of the same information.

The complaint stemmed from Grey House's collection, use and disclosure of an individual's personal information, which it shared with ESDC under a services contract between Grey House and the Department. Grey House was required to supply an email distribution list to the Department with more than 40,000 email addresses, some of them linked to associations and non-profit organizations. The complainant's name, email address and phone number – which Grey House had obtained from a website listing the complainant as a contact person for the local "circle" or chapter of a national non-profit association – were provided to ESDC.

The Department used Grey House's list to send unsolicited emails promoting the Prime Minister's Volunteer Awards, a program it administers, to the complainant. The complainant alleged that this information had been collected and shared by Grey House without his knowledge and consent. Despite the lack of consent, the ESDC email stated, erroneously, that recipients of the message had been identified as subscribers to a list owned by Grey House. The complainant had also requested that ESDC remove his name from its mailing list the previous year, but it had failed to do so and did not inform Grey House of the request.

We noted that ESDC's contract with Grey House stipulated that the contact information was to have been collected in accordance with Canadian legislation and with all necessary consents. In this case, the complainant's contact information had been collected by Grey House without his knowledge or consent, in contravention of PIPEDA, and in a manner violating the terms of the contract. Given that it was ESDC's responsibility to ensure that Grey House complied with the terms of the contract, the collection of the complainant's contact information fell outside the parameters stipulated by ESDC for the program. Accordingly, we found that it had been collected in contravention of section 4 of the *Privacy Act*.

The complainant's name has since been removed from the ESDC email distribution list and he has received no further mailings related to the awards from the Department. In addition, ESDC has made amendments to its processes to guard against any future reoccurrence.

Related documents

Report of findings related to the investigation into ESDC

Case summary related to the investigation into Grey House

Early resolution success story

An individual filed a request to obtain access to his personal information from a federal institution but was told that the institution did not have the information he was seeking. Dissatisfied, the individual made a complaint to our Office. An investigator from our Office contacted the institution and confirmed it did not hold the information. After a few phone calls, our investigator was able to identify the institution that did have the information and confirmed it could process the individual's request. The investigator shared this information with the individual, who was then able to submit a new request for access to his personal information to the correct institution.

This case underlines the value of the early resolution of the matter relative to the time-consuming process of a complaint investigation. Addressing privacy issues upfront and resolving matters cooperatively, outside formal enforcement, is our preferred approach where appropriate.

Breach reporting update

The number of data breaches reported by public institutions dropped significantly in 2018-2019 – down by 46%. Our Office received only 155 public sector breach reports, far fewer than the 286 reports received in 2017-2018.

Breach report numbers have fluctuated significantly since May 2014, when a Treasury Board directive made it mandatory to report "material" breaches to our Office.

There are strong indications of systemic under-reporting of certain types of breaches across government. The vast majority of the breach reports received by our Office (84%) pertain to data that has been lost or accidentally disclosed. While there is no evidence to suggest that the public sector is immune to cyber breaches, few cyber breaches have ever been reported to us by the public sector. As well, in 2018-2019, we received only 17 breach reports related to unauthorized access to personal information.

Our review of government breach reporting in last year's report had raised a number of concerns about breach reporting in the public sector, including issues related to privacy accountability, information technology safeguards and the knowledge of front-line workers about what constitutes personal information.

For example, we found there was confusion over whether a Canadian passport represented sensitive personal information. In response to the specific issue of passports, we have now launched a small-scale audit into government passport management practices.

Many of the institutions in our review acknowledged their employees do not fully grasp what constitutes personal information and their obligations under the Act.

To follow up more broadly on the findings of our breach study, we urged TBS to strengthen its policy guidance and tools, raise awareness, and improve

training in the federal government. To that end, TBS has developed an action plan and is reporting on its progress. For instance, TBS has reported stronger engagement with stakeholders, meeting with key communities of practice, and developing training materials and tools aimed at federal government employees. At the time of drafting this report, we are continuing to monitor progress and await the opportunity to review specific documents and tools.

We are working with TBS towards creating an online breach reporting form that will help institutions provide more complete information when reporting a breach. It will also offer guidance on breach reporting requirements.

For many years, we have recommended that the *Privacy Act* be amended to make breach reporting mandatory. We believe there should be an explicit requirement for government institutions to report breaches of personal information to our Office in a timely manner and to notify affected individuals in appropriate cases.

There are many inconsistencies in how various government institutions are applying the Treasury Board guidelines. Placing a specific legal obligation on federal institutions to report privacy breaches to our Office would ensure we have a better picture of the current scope of the problem, and that we are consulted in the process of responding to breaches and mitigating their impact on individuals. Such a change would also avoid the disconnect between Canada's federal public and private-sector privacy laws.

Our Office uses the breach reports we receive from the public sector to ensure that Canadians' interests are appropriately considered and to help federal institutions mitigate harm to Canadians. They are invaluable in helping our Office to assess overall breach management practices and determine when and how to address privacy risks through advice and recommendations. It is therefore critical that breaches be appropriately reported to our Office.

Advice to federal institutions

Our Office's Government Advisory Directorate completed its first full year of operations in 2018-2019. It provides advice and recommendations to federal public sector institutions in relation to specific programs and initiatives. The Directorate provides this advice through consultations as well as through the review of PIAs and information-sharing agreements submitted by departments and agencies.

The Directorate also undertakes various outreach initiatives with the federal public sector in order to encourage compliance with the *Privacy Act*. The goal is to share information and advice with departments when they are designing or modifying their services so that risks to Canadians' personal information are minimized, including during the design of new and innovative programs. The goal of the Directorate's advice is to support institutions in mitigating impacts to privacy as part of their program design, prior to implementation.

Addressing privacy matters proactively and cooperatively, outside of formal enforcement, avoids time-consuming and costly investigations. It also helps mitigate future privacy risks, offers institutions a measure of consistency and predictability in their dealings with our Office and helps ensure the benefits of technological innovation outweigh the risks.

While the Office has been providing federal institutions with informal advice and reviewing PIAs for many years, the Directorate was established at an opportune time. The Government of Canada has committed to increasing its use of digital services as well as leveraging innovative ways to use and share data in order to deliver programs and services to Canadians more efficiently. Unsurprisingly, the number of proactive consultation requests received from government institutions has doubled in the first year of existence of the Government Advisory Directorate.

Recommendations on digital government initiatives

- Legislative authority is required to collect and share personal information, and accountability for the governance of personal information must be clear and documented.
- Institutions should collect only the information that is necessary for the delivery of the program or service.
- Safeguards such as access controls and breach prevention should be built in from the start and in place before implementation.
- Government employees' roles and responsibilities to protect privacy should be clearly documented and well understood.
- Institutions should be transparent about how they collect, use and share personal information, including how it may be combined, matched, analyzed and evaluated to create new data.
- Our Office should be consulted early in the development process, so we can give meaningful privacy advice before new programs or activities are implemented.

Over the past year, the Government Advisory Directorate offered advice on a range of digital government initiatives and innovations. We consulted with institutions on the development and use of advanced and predictive analytics, which is increasing across government.

We also offered advice on programs for identity authentication and verification, including the "tell us once" approach and plans for the development of a single, trusted digital identity for individuals to access multiple government services and accounts. We also provided advice on the expansion of online applications for immigration and social services, taxes, and pensions.

We consulted with the Canada Revenue Agency (CRA), ESDC and TBS on a program that allows individuals to access both CRA's My Account service and ESDC's My Service Canada Account online by signing into either one. Users would be able to use a single login credential to view information and make changes in a single session.

We also engaged with the CRA and ESDC on the Direct Deposit and Address Information Sharing Initiative. Through this program, Canada Pension Plan recipients provide or update their direct deposit information to one department. The information is then shared and used by both organizations for all benefit and tax credit programs administered by either agency.

In addition, we provided advice on a variety of innovative uses of technology, data collection and analysis across government, such as the initiatives highlighted below.

TBS Talent Cloud Staffing Platform

TBS is leading the Talent Cloud Staffing Platform initiative for federal institutions seeking to hire individuals for project-based term positions. TBS submitted a PIA to our Office covering the first phase of Talent Cloud.

In our review of the PIA, we expressed concerns about job applicants having the option to provide biographical information in open-text fields. This creates risks for over-collection of personal information including sensitive personal information.

We also recommended that TBS provide applicants' personal information to hiring departments in a secure manner, governed by information sharing agreements clearly outlining terms and conditions regarding sharing. TBS has been receptive to our recommendations and indicated it will incorporate our feedback as the initiative progresses. Talent Cloud is currently in a pilot stage. Future phases include an Indigenous talent portal, a hiring model using bias-reduction tools, and verification of online applicants' credentials using blockchain technology. TBS anticipates submitting two more PIAs related to these plans.

TBS Next Generation Human Resources and Pay Initiative

TBS is leading the Next Generation Human Resources and Pay initiative, which is exploring a solution to human resources and employee pay for the federal public service and undertaking stabilization of the Phoenix Pay System. Our Office is consulting with TBS and providing advice on the privacy requirements of these solutions.

During early consultations on possible solutions, we raised a concern about using personally identifiable data during the testing phase leading up to and during pilot projects. We recommended that TBS either first de-identify the data or enter into strong information sharing agreements with vendors to ensure data was anonymized. TBS assured us the data would not include personal identifiers and that confidentiality agreements would be put in place between TBS and potential vendors. We expect to receive a PIA for one or more pilot projects for this initiative.

RCMP Wide Awake social media monitoring

The RCMP's Wide Awake project uses a tool that analyzes content posted to social media to proactively identify threats to public safety so that the RCMP may intervene if necessary. Our Office met with the RCMP about this tool in its early design phase and recommended a PIA be conducted for the project. In response to our concerns about transparency, the RCMP advised us that it plans to make a summary of its policies on social media analysis available on its website. It noted that officers only access information on social media that is publicly available. We noted that, while the expectation of privacy attached to publicly available information is reduced, there is still a residual reasonable expectation of privacy that requires protection.

CBSA passenger information

In response to our receipt of numerous, narrowly-scoped PIAs relating to the use of passenger information, we asked the CBSA to provide our Office with a comprehensive overview of privacy risks associated with the collection, use, analysis and disclosure of air traveller information under the Advance Passenger Information / Passenger Name Record (API/PNR) program. The API/PNR program involves the collection of prescribed information from commercial air carriers to identify persons who are or who may be involved with terrorism or terrorism-related crimes or other serious crimes, including organized crime, that are transnational in nature.

The Agency has submitted an umbrella PIA that addresses the acquisition of this data, as well as a series of addenda PIAs for subsequent uses of the data.

The suite of PIAs included descriptions of the initial data acquisition, the analysis of the information, targeting of air travellers, and the development of intelligence products and disclosure of information generated from the data, including under the Scenario Based Targeting program, which was the subject of a Review by our Office in 2017.

We have previously discussed the necessity and proportionality of the Scenario Based Targeting program with the CBSA. We have expressed concerns about the risk scenarios, which are made up of personal characteristics derived from API/PNR, such as age, gender, travel document origin, itinerary and length and pattern of travel. These factors are used to analyze traveller information and to target individuals arriving in Canada for further scrutiny.

During our 2017 review of the Scenario Based Targeting program, we recommended that scenarios should be reviewed for privacy, human rights and civil liberties impacts prior to being launched and on an ongoing basis. We advised that decisions made to modify or delete scenarios based on such reviews should be clearly documented. In addition, we recommended that scenarios that do not meet criteria for effectiveness should be amended or deleted.

It is our understanding from the CBSA Advance Passenger Information / Passenger Name Record Program / Air Passenger Targeting PIA that the Agency updated its governance framework for evaluating scenarios used in Scenario Based Targeting in March 2018. The PIA indicates this measure was taken in response to our 2017 PIA review, which called for a documented evaluation process to assess the potential impacts on privacy, civil liberties and human rights.

During the 2017 Scenario Based Targeting review, we also raised concerns that individuals not found to be threats under the API/PNR program may have their information disclosed to domestic and foreign partners early in the review process. This creates a risk that such information may be unnecessarily retained or disclosed onward. We recommended the CBSA review its information-sharing agreements with partners with this risk in mind. CBSA agreed to undertake an internal review of key information sharing agreements; the PIA submitted to us in 2018 includes this review. We continue to consult with the CBSA on this program.

Privacy Commissioner Alerts

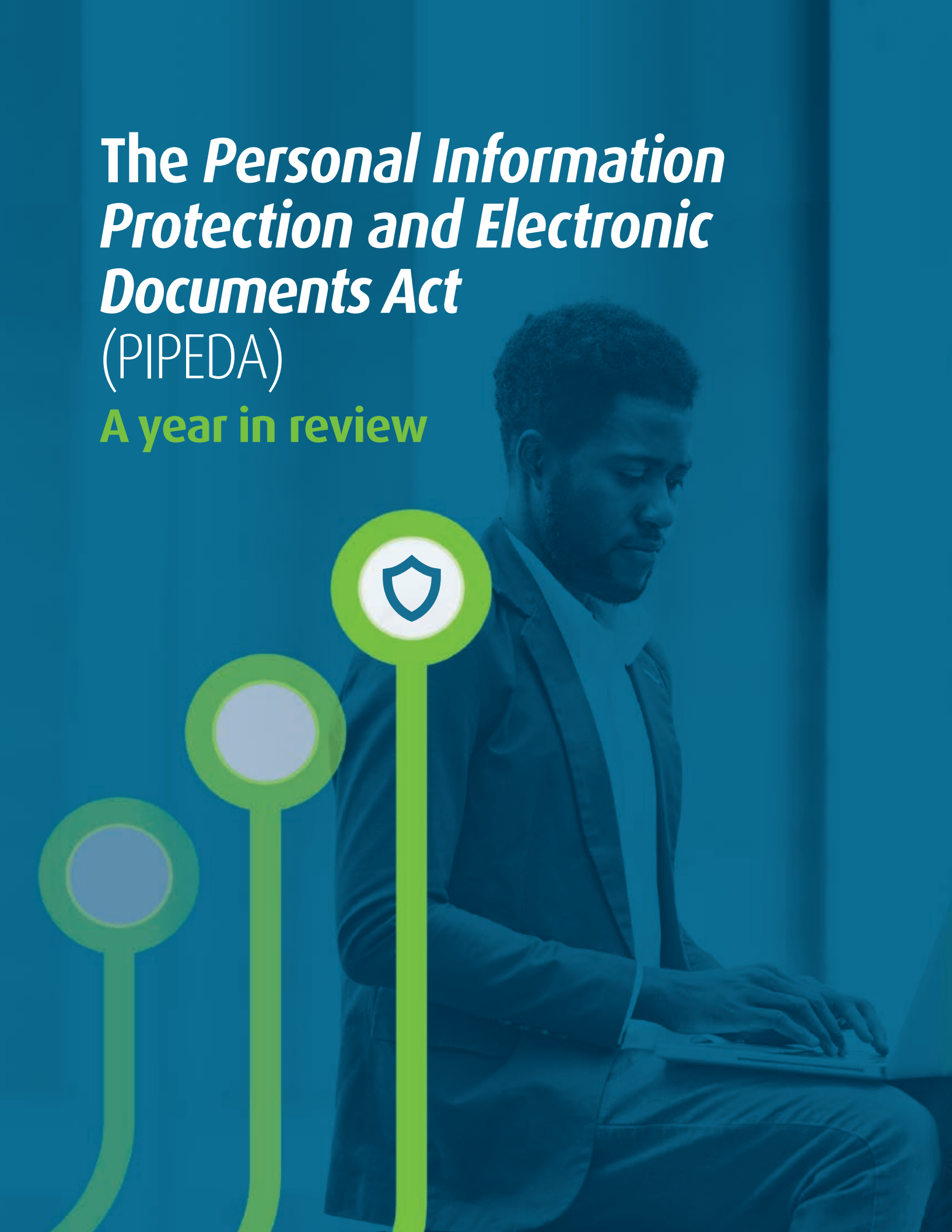
A new initiative launched in 2018-2019 was the Privacy Commissioner Alerts, sent via email, which allow our Office to share important privacy news, trends, best practices and key takeaways from our work with ATIP coordinators as issues and trends arise.

At the time of drafting this report, alerts had been issued regarding the use of portable storage devices, outsourcing to third parties, and the importance of proper retention practices in mitigating potential privacy breaches.

We know there are many lessons to be learned from our investigations, privacy breaches reported to our Office, our reviews of PIAs and our advisory work with government institutions. Confidentiality provisions in the *Privacy Act* can make it challenging to share many of these lessons with the wider federal public service in a timely, efficient way. Privacy Commissioner Alerts allow our Office to communicate these lessons to federal government institutions while maintaining our confidentiality obligations.

The *Personal Information Protection and Electronic Documents Act* (PIPEDA)

A year in review



Our Office's work related to PIPEDA covers a wide array of activities. It includes investigating complaints, monitoring compliance with our recommendations, collaborating with other organizations responsible for enforcing Canada's Anti-Spam Law (CASL), receiving and examining breach reports, and providing advice and guidance to businesses as they continue to look to the potential of the digital age to provide new products and services to consumers.

The most prominent investigations we conducted under PIPEDA in 2018-2019 were about the Facebook / Cambridge Analytica scandal and the Equifax data breach. These and other cases summarized in this section attest to the failings of accountability and safeguards in current business models, and support our case for legislative reform.

Mandatory breach reporting also came into effect during the past year, providing our Office with better insight into the types of breaches that are occurring and the risks facing Canadian businesses.

Operational updates and trends

This past year, we closed 282 complaint files, including 178 through early resolution.

Early resolution continues to be an efficient mechanism to resolve straightforward privacy matters, typically taking an average of less than three months, compared to more than a year for a formal investigation process.

Complaints that are not resolved through early resolution increasingly involve emerging technologies, novel business models with multi-jurisdictional implications, and issues that cross-cut privacy and other areas, such as consumer protection.

Despite a concerted effort to close older complaints, our backlog has continued to grow. At the end of 2018-2019, our inventory of active PIPEDA investigations older than 12 months – most of them involving more complex issues – grew from 55 to 64, representing a 16% increase.

Temporary funding announced in the 2019 federal budget to address our backlog will increase our capacity over the next two years to deal with older complaints.

Organizations in the financial sector continue to be the target of a significant proportion of the complaints we accept (20%). Other top sectors for complaints included telecommunications (13%), services (11%), Internet (10%) and transportation (10%). Investigations into these five sectors collectively made up almost two-thirds of all complaints accepted.

As in recent years, Canadians are most likely to complain about issues related to access to their personal information (29%). Issues of use and disclosure of personal information (18%) and consent (17%) were also popular concerns.

Facebook refuses to address privacy deficiencies

The Office's investigation of Facebook in relation to the Cambridge Analytica scandal ended with the social media giant's deeply disappointing decision not to implement recommendations aimed at correcting serious privacy deficiencies.

As discussed earlier in this report, the case highlights the urgent need for legislative reform.

The investigation – conducted jointly with the Office of the Information and Privacy Commissioner for British Columbia (BC OIPC) – found that Facebook had committed serious contraventions of Canadian privacy laws.

Commissioner Therrien noted a stark contradiction between Facebook's public promises to improve its privacy practices and its refusal to address concerns identified during the investigation.

The complaint that initiated the investigation followed media reports that Facebook had allowed an organization to use an app to access users' personal information and that some of the data was then shared with other organizations, including Cambridge Analytica, which was involved in political campaigns in the US and the UK.

The app encouraged users to complete a personality quiz. It collected information about users who installed the app as well as their Facebook "friends." Some 300,000 Facebook users worldwide added the app, leading to the potential disclosure of the personal information of approximately 87 million others, including more than 600,000 Canadians.

Some of the key findings of the investigation were that:

- Facebook's superficial and ineffective safeguards and consent mechanisms resulted in a third-party app's unauthorized access to the information of millions of Facebook users. Some of that information was subsequently used for political purposes.
- Facebook failed to obtain meaningful consent from both the users who installed the app as well as those users' "friends," whose personal information Facebook also disclosed.
- Facebook did not exercise proper oversight with respect to the privacy practices of apps on its platform. It relied on contractual terms with apps to protect against unauthorized access to user information; however, its approach to monitoring compliance with those terms was wholly inadequate.
- There was an overall lack of responsibility for personal information at Facebook. Rather, Facebook attempted to shift responsibility for protecting personal information to the apps on its platform, as well as to users themselves, even though a basic principle of privacy laws is that organizations are responsible for the personal information under their control.

The fact that Facebook said it would not implement recommendations to address those issues leaves a high risk that the personal information of Canadians could be used in ways that they do not know or suspect, exposing them to potential harms. This is extremely worrisome given the vast amount of sensitive information people have entrusted to Facebook.

For these reasons, our Office announced its intention to apply to the Federal Court to seek a binding order to force the company to take action to correct its privacy practices.

Resolving this issue is vital. It is untenable that organizations can ignore our Office's legal findings. Facebook should not get to decide how Canadian privacy laws are interpreted.

Report of findings

Investigation into Facebook

Security shortcomings led to massive breach at Equifax

An investigation by our Office found a series of unacceptable security deficiencies by Equifax that paved the way for a massive global data breach and exacerbated its impact.

Some 143 million people worldwide – including 19,000 Canadians – were affected by the breach at this credit reporting agency.

Hackers gained access to Equifax Inc.'s systems in May 2017 by exploiting a known vulnerability in a software platform. The attackers were able to operate undetected within Equifax's system for 77 days. The company had been aware of the vulnerability for more than two months but had failed to fix it.

It was unacceptable to find such significant shortcomings in privacy and security practices in a company that holds a vast amount of highly sensitive personal information and plays a pivotal role in the financial sector.

Our Office received 19 complaints against Equifax following the breach. We conducted a two-pronged investigation that examined both Equifax Canada and its US-based parent company, Equifax Inc.

The investigation highlighted a range of deficiencies in Equifax Inc.'s security program, including:

- inadequate vulnerability management to prevent attacks through known vulnerabilities;
- inadequate network segregation to reduce the scope of access and harm in the case of a breach; and
- inadequate implementation of basic information security practices to appropriately manage the use of personal information and identify potential unauthorized use.

Critically, the investigation highlighted failures by both Equifax Canada and its parent company to adopt oversight mechanisms that should have been in place to accurately assess the security risks faced and ensure that the security program was adequate to protect the sensitive personal information held by Equifax Inc. against those risks.

The personal information of Canadians was caught up in the breach at US-based Equifax Inc. because these Canadians had obtained products, such as credit monitoring or fraud alerts, from Equifax Canada – transactions that were processed by its parent company.

Several complainants told our Office they were surprised to learn their information had left Canada and was transferred to the US.

We found the transfer to be inconsistent with the organization's obligation under PIPEDA to obtain meaningful consent from individuals before disclosing their personal information to a third party. For consent to be valid, individuals must be provided with clear information about the disclosure, including when the third party is located in another country, and the associated risks.

Since the breach, Equifax has taken a number of steps to improve their security and accountability programs. It has entered into a binding compliance agreement to complete additional remediation and submit third-party audit reports on Equifax Canada and Equifax Inc's security to our Office every two years for a six-year period. This will enable ongoing monitoring of compliance with PIPEDA.

While Equifax Canada ultimately agreed to offer free credit monitoring to breach victims for a minimum of four years, the company did not go so far as its parent company in regard to other post breach protections. Affected consumers in the US were offered a credit freeze allowing them to

restrict access to their credit files, thus reducing the chance of fraudulent or unauthorized credit checks.

Report of findings

Investigation into Equifax

Other key investigations

World Anti-Doping Agency (WADA) completes implementation of investigation recommendations

In our 2017-2018 Annual Report, we discussed the findings of an investigation into a breach involving the Montreal-based WADA, which oversees the international anti-doping regime for amateur sports.

The breach involved a hacker group known as Fancy Bear that accessed the Agency's anti-doping database. The Fancy Bear group has been identified by national governments, including Canada, as a cyberespionage operative of the Russian state through its intelligence arm, the GRU.

The Fancy Bear group disclosed the health information of more than 100 athletes who competed in the 2016 Rio Olympic Games. The information disclosed included medical conditions, medications and analyses of bodily specimens. WADA's database contains additional sensitive information such as genetic information and details on athletes' whereabouts.

Our investigation found that the Montreal-based Agency had failed to implement a security framework in line with its status as a high-value target for hackers, including state-sponsored groups. Deficient security measures left the Agency vulnerable to an attack that began as a phishing campaign in which hackers sent emails to WADA employees and other individuals with access to the database.

At the conclusion of our investigation, WADA agreed to implement all of our recommendations. We entered into a compliance agreement with WADA in order to monitor the organization's implementation of our recommendations.

This year, we can report that WADA has implemented the recommendations to our satisfaction.

The report of findings for WADA is now available. The report and the investigation offer valuable lessons and insights to other high-profile organizations, including:

- applying higher levels of protection to highly sensitive information or information that may be otherwise valuable to hackers;
- having robust access controls, such as two-factor authentication, mandatory password changes and an alert system to notify users when unusual activity on their accounts is detected;
- encrypting data when it is stored, not only when it is in transit;
- ensuring the information security framework is comprehensive and includes written policies, procedures and training; and
- communicating to staff, through training or other means, information about security awareness.

Related documents

Report of findings related to WADA

Compliance agreement with WADA

Early resolution success story

A complainant filed an accuracy complaint against a bank, alleging that the bank erroneously continued to report his social insurance number on his mother's T5 slips to the CRA despite his repeated requests for correction. This resulted in him having to file reassessments for income that was not his. After our investigator contacted the bank, the root cause of the problem was identified and corrected. Our Office also facilitated a discussion between the complainant and the bank, which brought the matter to a close.

Online telephone directory charged fees for removal of numbers

411Numbers HK Ltd. (411Numbers), a company incorporated in Hong Kong but operated from Quebec, oversaw more than a dozen websites that provided free access to telephone numbers and other information about individuals in Canada and other countries. It generates revenues through advertising and previously made money by charging a fee to remove such information.

The complainant alleged that 411Numbers collected, used and disclosed his name, address and unlisted phone number without his knowledge and consent when it posted this personal information on its website. He also objected to 411Numbers using his information to generate revenue through a paid removal service and requiring individuals to provide more information than necessary to use the removal service. To delete personal information from the website, the company demanded copies of a passport, driver's license and utility bill. In addition, the complainant accused the firm of being unresponsive to his privacy-related questions, a claim substantiated by our Office as we also initially had great difficulty contacting the business.

411Numbers asserted our Office did not have jurisdiction to investigate this matter because the company was incorporated under the laws of Hong Kong and its servers were located outside Canada. However, the investigation found that there was a real and substantial connection between 411Numbers' operations and Canada, based on evidence we uncovered that its activities were effectively carried out from Canada.

The company also argued that the information in question was publicly available, so consent was not required to post it on its websites. Our Office rejected this argument. While names, addresses and telephone numbers published in a telecommunications company's white-pages directory are publicly available, unlisted telephone numbers are not, so individuals' consent to collect, use and disclose such information is needed.

In response to this investigation, the complainant's personal information was removed from the website and 411Numbers ended its practice of removing information for a fee. Individuals asking to have their information erased from the listing service now only need to complete an online form. Since the company ceased charging for removal, we considered that aspect of the matter resolved, but we also noted that the publication of personal information, without consent, for the purposes of encouraging individuals to pay to have it removed would likely be considered inappropriate under PIPEDA.

Finally, we found that individuals had great difficulty contacting 411Numbers, that the company was insufficiently aware of its obligations under PIPEDA and that its privacy policy contained multiple errors.

Our Office made several recommendations that 411Numbers agreed to implement. It committed to:

- remove the data associated with unlisted numbers on all its websites;
- implement due diligence measures to ensure listings obtained in the future do not contain unlisted numbers; and
- implement measures to enhance its accountability, openness and ability to respond to individuals' wishing to challenge its compliance with the Act.

During our investigation, we received a request for assistance from a European data protection authority that had received similar complaints against 411Numbers from several individuals. As a result of our investigation, 411Numbers also agreed to remove those individuals' personal information from the site.

Ultimately, we note that at the time of drafting this report, none of 411Numbers' non-Canadian websites are in service, the information of more than one million Canadians has been removed from the company's Canadian website, and we are still in contact with the organization to ensure full implementation of all of our recommendations.

Report of findings

Investigation into 411Numbers

Canada's Anti-Spam Law (CASL)

Our Office shares responsibility for enforcing CASL with the Canadian Radio-television and Telecommunications Commission (CRTC) and the federal Competition Bureau. All enforcement agencies worked collaboratively and met regularly with domestic and international partners in order to promote compliance with CASL in the past year.

Last year, our Office worked alongside the other CASL enforcement agencies to support the launch and publication of a new CASL Performance Measurement Report providing more helpful information to businesses, as well as a revamp of ISED's CASL-related website for the general public, fightspam.gc.ca.

Our Office is a member of the Unsolicited Communications Enforcement Network (UCENet), a network of anti-spam, consumer protection and telecommunications regulatory authorities. Our Office participated in discussions at a UCENet meeting to develop the network's 2019-2021 Operational Plan. Our Office also presented a technical study conducted in support of an adware investigation, and an update on its CASL-related mandate and activities at the 2018 joint annual meetings of UCENet and the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG), which was attended by private sector IT security experts.

Our Office delivered ongoing CASL-related compliance guidance for businesses and advice for individuals through different channels. In 2019-2020, our Office updated its online resources related to CASL, including compliance help for businesses and a general webpage on CASL. Our Office also launched and promoted a new presentation package on PIPEDA for businesses, which offers information about CASL and how the law relates to e-marketing practices. Our Office also exhibited and spoke at a number of events about CASL and distributed related materials to businesses.

Our Office's Information Centre received 78 CASL-related inquiries from individuals and businesses. The top three types of inquiries related to reports of unsolicited messages; questions about unsubscribing from email distribution lists; and general questions about the applicability of CASL and how to achieve compliance.

Breach reporting update

November 1, 2018, marked the beginning of a mandatory breach reporting regime under PIPEDA. Since then, we have seen breach report volumes increase by almost 500%.

In terms of trends, we are seeing a rise in reports of breaches affecting a small number of individuals – often just one and sometimes through a targeted attack. Organizations must now report any breach that meets the reporting threshold under the regime, regardless of the number of individuals affected. Under the previous voluntary regime, we received relatively few breach reports where only a small number of people were affected.

The majority of reported breaches involve unauthorized access (62%) – that is to say they are perpetrated by malicious actors or employees snooping. Early analysis reveals that employee snooping and social engineering hacks are the trending causes for breaches resulting from unauthorized access. Social engineering hacks involve targeted phishing and impersonation schemes, sometimes using personal information or credentials leaked from previous breaches, in attempts to take over another individual's accounts for financial gain.

We are also continuing to see breaches involving disclosure to family members, theft and loss of devices, malware insertion, attacks on network vulnerabilities, credential stuffing, brute force password attacks, and accidental disclosures (such as including lists of email recipients in the c.c. field instead of the b.c.c. field), among others.

However, in many cases, businesses may be erring on the side of caution and reporting breaches that do not appear to meet the reporting threshold of a "real risk of significant harm." In fact, 33% of the breaches reported from November 2018 to the end of March 2019 did not appear to meet that threshold. While each case has to be assessed on its own merits, in some instances, organizations reported breaches where no personal information was actually at play, or where an attempt of a bad actor to breach security safeguards was unsuccessful.

Our Office developed guidance to help organizations comply with their new obligations, which cover general issues such as determining what steps to take in the event of a breach, creating breach records, and notifying affected individuals.

At the time of writing this report, we have undertaken breach record inspections as a first on-the-ground litmus test of the state of compliance with mandatory breach obligations. In addition to enforcing compliance, this exercise will give us insight into issues for which guidance might be appropriate, such as how real risk of significant harm should be interpreted, under-reporting, and improper record-keeping.

Advice to businesses

Our Office's Business Advisory Directorate was created in 2018 as a means to help businesses better understand the privacy implications of new technologies and business models before these are deployed in the marketplace, or to assist them in assessing the privacy implications of their current practices.

While we feel stronger enforcement powers should be part of a modern legislative framework, enforcement should not be the primary strategy to seek compliance. The creation of the Business Advisory Directorate is part of an overall shift of our activities towards greater proactive efforts.

Addressing privacy issues upfront and resolving matters cooperatively, outside formal enforcement, remains our preferred approach. It avoids time-consuming and costly investigations, helps mitigate future privacy risks, offers organizations a measure of consistency and predictability in their dealings with our Office and allows everyone to benefit from innovation.

The Directorate may proactively offer its advisory services; however, all businesses subject to PIPEDA can request a consultation with our experts. The reaction from the private sector has so far been positive.

This past year, our Office issued guidance, met with privacy leaders from a variety of commercial enterprises, and explained best practices that businesses can employ to obtain the meaningful consent necessary to use customer data and limit inappropriate data collection.

Our Office's business advisory engagements generally remain subject to PIPEDA's confidentiality provisions. In appropriate select cases, some information may be disclosed if it is in the public interest. The following are such cases that illustrate the work done by our Office's Business Advisory Directorate in 2018-2019.

Apple Maps Project

Apple Inc.'s active Maps Image Collection project for street cartography and mapping is being conducted in various countries, including Canada, to collect data for improving Apple Maps. Apple voluntarily sought a business advisory consultation with our Office regarding this project. While details of the discussions cannot be shared due to the confidentiality provisions of PIPEDA, we can report that Apple has been receptive to our initial recommendations and remains engaged in discussions with our Office.

Sidewalk Labs' Quayside Project, Toronto

Manhattan-based Sidewalk Labs plans to develop a 12-acre district on Toronto's waterfront known as Quayside in partnership with Waterfront Toronto, a corporation created and funded by three levels of government. Sidewalk Labs is affiliated with Alphabet Inc., Google's parent company.

The potential privacy implications of this technology driven project have been widely covered in the national media, with critics divided on whether the expected benefits of the initiative with respect to sustainability and quality of life would outweigh its potential for mass surveillance of Canadian citizens by an American technology giant.

Our Office is currently reviewing the project's Master Innovation and Development Plan released by Waterfront Toronto in June 2019, and where appropriate, we will provide our comments and recommendations on aspects of the plan that would fall under PIPEDA. Given the ground-breaking nature of this project and its significance for the future of urban design in Canada and beyond, our Office continues to monitor developments and proactively engage with the relevant parties to provide our input and advice, as relevant.

Contributions Program

Our Office funds independent privacy research and related knowledge translation initiatives through its Contributions Program. The goal of the program is to generate new ideas, approaches and knowledge about privacy that organizations can apply to better safeguard personal information and that individual Canadians can use to make more informed decisions about protecting their privacy.

Each fall we issue an annual call for proposals, and academic institutions as well as non-profit organizations are eligible for funding. This includes industry associations, consumer and voluntary organizations, trade associations and advocacy organizations. The budget is $500,000 annually.

Our Office received 29 proposals for the 2018-2019 funding cycle. These proposals were evaluated by the Office, as well as by an external peer-review panel. In the end, nine successful projects were selected to receive funding support.

In 2018-2019, the projects we funded touched on a wide range of issues, including:

- a study by the University of Toronto on stalkerware, a kind of intrusive surveillance software that a person installs on another person's device and uses to facilitate intimate partner harassment or violence;
- a study by McMaster University that provides a deeper understanding of the privacy implications of smart cities in Canada;
- a study by Option consommateurs that explores the privacy implications of parents' posting of their children's information and pictures on social media;
- a project by the BC Society of Transition Houses aimed at providing guidance to Canadian women's and children's anti-violence organizations about critical privacy and security considerations relating to the use of electronic databases in the course of their activities; and
- a study by Concordia University on privacy leakage in Canadian public Wi-Fi networks.

The independent research we fund through the Program informs the work we do at the Office. For instance, a 2018 research project by the Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC) on the privacy implications of Canada's data broker industry, has informed an investigation we are conducting on that industry.

Privacy cases in the courts

Union of Canadian Correctional Officers-Syndicat des agents correctionnels du Canada – CSN (UCCO-SACC-CSN) v. PGC - A-463-16 (Federal Court of Appeal)

This is an appeal by the Union of the Canadian Correctional Officers of the Federal Court's decision in 2016 FC 1289. In this case, the Federal Court found that mandatory credit checks for correctional officers, as required by a new TBS Standard on Security Screening ("the Standard"), did not contravene the *Privacy Act* or the *Canadian Charter of Rights and Freedoms*. The Federal Court also found that section 4 of the *Privacy Act* did not require that the collection of personal information be **necessary** for a government institution's operating programs or activities.

Our Office was granted leave to intervene in the appeal, and made arguments concerning the interpretation of section 4 of the *Privacy Act*, namely that it does impose a necessity threshold upon government institutions for the collection of personal information, and whether the union was permitted to raise a section 4 violation by way of judicial review.

R. v. Jarvis, 2019 SCC 10

This case concerns a high school teacher who used a camera pen to make surreptitious recordings of multiple female students at the school where he taught, many of which focused on the students' chest area and cleavage. The teacher was charged with voyeurism under subsection 162(1) of the *Criminal Code*, but was acquitted at trial on the basis that the Crown had not proven beyond a reasonable doubt that the recordings had been made for a "sexual purpose".

On appeal, the Ontario Court of Appeal was unanimous in finding that the recordings had been made for a "sexual purpose". However, the majority concluded that the recordings had not been made "in circumstances that give rise to a reasonable expectation of privacy", and therefore this element of the voyeurism offence had not been made out. The majority's reasoning hinged on the fact that the students were in a public setting when the recordings were made (i.e., in and around the school) and therefore had to expect that they would be observed and recorded. In dissent, Huscroft JA concluded that the students did enjoy a reasonable expectation of privacy with respect to anyone who would seek to compromise their personal and sexual integrity while they are at school and would have allowed the appeal.

The Crown appealed the Ontario Court of Appeal's decision as of right to the Supreme Court of Canada on the basis of Huscroft JA's dissent.

Our Office, along with several other organizations, was granted leave to intervene. Our Office argued that the concept of a reasonable expectation of privacy in the context of the voyeurism offence must be assessed based on the totality of the

circumstances and that the narrow, location-based approach adopted by the majority of the Ontario Court of Appeal was incorrect and would undermine the privacy rights of Canadians in a range of contexts.

In its decision, the Supreme Court of Canada upheld a contextual understanding of privacy in public places in the context of the offence of voyeurism. The Court acknowledged that privacy is not an all or nothing concept, and that an individual does not forfeit all privacy rights simply because they are in a public or semi-public place.

In determining whether an individual's privacy interests have been invaded, the ruling also underscored the need to look at these matters on a case-by-case basis, taking into account all of the particular circumstances. In this regard, the Court reaffirmed that privacy must be evaluated in light of changing technologies, which can make it easier for the state and private entities to "glean, store and disseminate information" about individuals, and that privacy should not correspondingly shrink as a result.

More generally, the Court was sensitive to the important privacy interests at play – young people's bodies and their reasonable expectation to be free from being recorded for a sexual purpose by someone in a position of trust.

Google Reference (T-1779-18)

This is an application by the Privacy Commissioner of Canada pursuant to section 18.3 of the *Federal Courts Act* referring two questions for hearing and determination:

> Does Google LLC ("Google") in the operation of its search engine service, collect, use or disclose personal information in the course of commercial activities within the meaning of para. 4(1)(a) of PIPEDA when it indexes webpages and presents search results in response to searches of an individual's name?
>
> Is the operation of Google's search engine service excluded from the application of Part I of PIPEDA by virtue of para. 4(2)(c) of PIPEDA because it involves the collection, use or disclosure of personal information for journalistic, artistic or literary purposes and for no other purpose?

The questions arose in the context of a complaint from an individual alleging that Google is contravening PIPEDA by continuing to prominently display links to online news articles concerning him in search results when his name is searched using Google's search engine service. The complainant requested that Google remove the articles in question from results for searches of his name.

In its initial response to the complaint, Google took the position, in part, that PIPEDA does not apply to it in the circumstances. In order to resolve, as a first step, this jurisdictional issue, the Privacy Commissioner referred the above two questions regarding whether PIPEDA applies to Google's operation of it search engine to the Federal Court for determination before continuing with the investigation.

Shortly after the reference was filed, Google brought a motion seeking to have the reference expanded to deal with the issue of whether a potential requirement to remove links from its search results would violate section 2(b) of the *Canadian Charter of Rights and Freedoms*, or, alternatively, to have the reference struck. On April 16, 2019, the Court dismissed Google's motion. Google appealed this decision. The Court dismissed this appeal on July 22, 2019, and a decision on the merits is still pending at the time of drafting this report.

Our Office has indicated that it will not finalize its Draft Position Paper on Online Reputation until the conclusion of the referenced proceeding.

Canadian Coalition for Genetic Fairness v. Attorney General of Quebec et al. (SCC 38478)

This case concerns a reference by the Government of Quebec concerning the constitutionality of the *Genetic Non-Discrimination Act*, S.C. 2017, c. 3 ("GNDA"), which prohibits certain harmful practices relating to the collection, use and disclosure of genetic test results.

In particular, the GNDA creates stand-alone prohibitions relating to forced genetic testing and the collection, use and disclosure of genetic test results without consent (sections 1-7). It also amended the *Canada Labour Code* (section 8) and the *Canadian Human Rights Act* (sections 9-10) to protect federally regulated employees in relation to genetic testing and to protect against discrimination based on genetic characteristics.

Shortly after its passage, the Government of Quebec referred the constitutionality of ss. 1 to 7 of the GNDA (but not the amendments to the *Canada Labour Code* or to the *Canadian Human Rights Act*) to the Quebec Court of Appeal. The reference asks whether sections 1-7 of the GNDA exceeds Parliament's authority to make laws in relation to criminal matters under the *Constitution Act, 1867.*

The provisions of the GNDA at issue prohibit the following:

- Requiring an individual to undergo a genetic test as a condition of providing goods/services or of entering into/maintaining a contract or any of its terms, or refusing to engage in such activities because of a refusal to undergo such testing (section 3).
- Requiring an individual to disclose the results of a genetic test as a condition of engaging in one of the activities listed above, or refusing to engage in the activities because of the refusal to disclose these results (section 4).
- The collection, use or disclosure of the results of a genetic test without the written consent of the individual concerned by any person engaged in providing goods or services, or entering into or maintaining contracts with individuals (section 5).

Section 6 exempts health care practitioners and researchers from the application of sections 3 to 5. Section 7 makes it an offence to contravene sections 3 to 5, with the potential for fines and prison time.

In its decision, the Quebec Court of Appeal was unanimous in finding that the provisions at issue were *ultra vires* Parliament's power to enact laws in relation to criminal matters.

The Canadian Coalition for Genetic Fairness ("the Coalition"), an intervener before the Quebec Court of Appeal, filed an as-of-right appeal of the Court's decisions to the Supreme Court of Canada.

The Attorney General of Quebec and the Attorney General of Canada, which also did not support the constitutionality of the GNDA before the Quebec Court of Appeal, are respondents to the appeal. Our Office, as well as the Attorneys General of British Columbia and Saskatchewan, the Canadian Life and Health Insurance Association, the Canadian Human Rights Commission and the Canadian College of Medical Geneticists are intervening in the appeal.

At the time of drafting this report, the hearing of the appeal was tentatively scheduled for October 10, 2019.

Certain guidance documents issued by our Office relating to the collection, use and disclosure of genetic test results refer to the GNDA and will be updated after the Supreme Court has issued its decision in this matter.

International and domestic cooperation

Privacy is increasingly a global challenge in our digitized world, as borders are no longer a barrier to technology's beneficial – and detrimental – impacts. Vast amounts of personal information now travel continuously between jurisdictions around the world.

In an era of constant innovation and increasing technological complexity, international cooperation to form a coordinated front on common privacy issues is critical to protecting citizens' privacy rights. When we share responsibilities and workloads among privacy authorities, we expand each authority's reach. Collaboration enables partners to leverage the strengths of each country's individual legislation, including regulatory enforcement powers, to ensure stronger and more holistic compliance practices.

Data protection authorities cannot advance their privacy goals in isolation. Many developing nations and regions that are adopting new privacy laws, or are in the process of creating privacy regulatory regimes, are reaching out to established jurisdictions such as Canada for assistance and information about best practices.

Taking part in these types of global initiatives ultimately helps to better protect Canadians. Stronger privacy rights in other parts of the world help ensure that Canadians are better protected when their personal information is sent outside of Canada's borders for processing.

In December 2018, Commissioner Therrien participated in a United Nations Security Council Counter-Terrorism Committee meeting in New York. The event discussed the challenges associated with protecting privacy and personal information while effectively combatting terrorism.

The Commissioner's remarks stressed that privacy is an internationally recognized human right and that counterterrorism measures involving the collection, sharing and analysis of personal information must respect that right. His speech also highlighted the importance of necessity, proportionality and independent oversight – principles that are central to most data protection and privacy laws, and particularly relevant in the context of national security.

Our Office regularly collaborates with privacy regulators from other countries. In some cases, we assist in sharing evidence to support unilateral enforcement action, in other cases we have partnered with authorities through jointly conducted investigations. For instance, in the last year, our investigation into 411Numbers was able to address the privacy concerns of individuals who submitted complaints to the German data protection authority.

In the case of Equifax, our Office benefited from collaboration with the US Federal Trade Commission and the UK Information Commissioner's Office (ICO). Although not technically joint investigations, we shared information with both organizations during the process of conducting our analysis. Similarly, our investigation into Facebook made use of information sharing with the UK ICO.

Robust relationships are equally integral to the work we do domestically. We have formalized agreements to consult and share relevant information with privacy commissioners in several provinces. This includes Memorandums of Understanding with the Office of the Information and Privacy Commissioner of Alberta (AB OIPC), the BC OIPC and the Information and Privacy Commissioner of Ontario. These agreements help to ensure that the system of privacy controls and protections for Canadians is as seamless as possible. For example, the BC OIPC consented to our request to adapt for our own use the provincial guidance on protecting privacy in the context of cannabis transactions following the legalization of marijuana in Canada.

Last year, we engaged in a greater number of collaborative investigations with domestic partners than ever before. Our Office's investigation into Facebook, Inc. was conducted jointly with the BC OIPC. We are also currently investigating the use of facial recognition technology in shopping malls being carried out with the AB OIPC, the BC OIPC and the Commission d'accès à l'information du Québec.

Our Office also strives to work collaboratively with its provincial and territorial counterparts on common public education and policy matters in the public and private sector. As we are all united in the effort to protect and promote privacy rights, we occasionally issue joint resolutions to highlight consensus on matters of public policy, outline shared concerns or support on certain issues of concern to Canadians. This alignment amongst domestic Information and Privacy Commissioners provides a benefit to Canadians by calling for action that will encourage consistent privacy protections for individuals across the country.

At the 2018 Annual Meeting of the Federal, Provincial and Territorial Information and Privacy Commissioners in Regina, Saskatchewan in September 2018, we supported a joint resolution calling on governments to pass legislation requiring political parties to comply with globally recognized privacy principles. The resolution also calls for legislation that provides Canadians with access to the personal information political parties hold about them and to provide for independent oversight to verify and enforce privacy compliance.

The resolution highlights the inconsistent coverage of political parties in Canada, and calls on government to legislate oversight of information practices that have the potential to significantly impact the privacy of citizens and undermine their trust in the democratic system. The resolution has supplemented our Office's comments on this matter and the need for law reform before ETHI on the study of the breach of personal information involving Cambridge Analytica and Facebook. This informs parliamentarians and helps guide them to further protect Canadians' privacy rights.

Appendix 1: Definitions

Complaint types

Access

The institution/organization is alleged to have denied one or more individuals access to their personal information as requested through a formal access request.

Accountability

Under PIPEDA, an organization has failed to exercise responsibility for personal information in its possession or custody, or has failed to identify an individual responsible for overseeing its compliance with the Act.

Accuracy

The institution/organization is alleged to have failed to take all reasonable steps to ensure that personal information that is used is accurate, up-to-date and complete.

Challenging compliance

Under PIPEDA, an organization has failed to put procedures or policies in place that allow an individual to challenge its compliance with the Act, or has failed to follow its own procedures and policies.

Collection

The institution/organization is alleged to have collected personal information that is not necessary, or has collected it by unfair or unlawful means.

Consent

Under PIPEDA, an organization has collected, used or disclosed personal information without valid consent, or has made the provisions of a good or service conditional on individuals consenting to an unreasonable collection, use, or disclosure.

Correction/notation (access)

The institution/organization is alleged to have failed to correct personal information or has not placed a notation on the file in the instances where it disagrees with the requested correction.

Correction/notation (time limit)

Under the *Privacy Act*, the institution is alleged to have failed to correct personal information or has not placed a notation on the file within 30 days of receipt of a request for correction.

Extension notice

Under the *Privacy Act*, the institution is alleged to have not provided an appropriate rationale for an extension of the time limit, applied for the extension after the initial 30 days had been exceeded, or, applied a due date more than 60 days from date of receipt.

Fee

The institution/organization is alleged to have inappropriately requested fees in an access to personal information request.

Identifying purposes

Under PIPEDA, an organization has failed to identify the purposes for which personal information is collected at or before the time the information is collected.

Index

Info Source (a federal government directory that describes each institution and the information banks – groups of files on the same subject – held by that particular institution) is alleged to not adequately describe the personal information holdings of an institution.

Language

In a request under the *Privacy Act*, personal information is alleged to have not been provided in the official language of choice.

Openness

Under PIPEDA, an organization has failed to make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Retention (and disposal)

The institution/organization is alleged to have failed to keep personal information in accordance with the relevant retention period: either destroyed too soon or kept too long.

Safeguards

Under PIPEDA, an organization has failed to protect personal information with appropriate security safeguard.

Time limits

Under the *Privacy Act*, the institution is alleged to have not responded within the statutory limits.

Use and disclosure

The institution/organization is alleged to have used or disclosed personal information without the consent of the individual or outside permissible uses and disclosures allowed in legislation.

Dispositions

Well-founded

The institution or organization contravened a provision of the *Privacy Act* or PIPEDA.

Well-founded and resolved

The institution or organization contravened a provision of the *Privacy Act* or PIPEDA but has since taken corrective measures to resolve the issue to the satisfaction of the OPC.

Well-founded and conditionally resolved

The institution or organization contravened a provision of the *Privacy Act* or PIPEDA. The institution or organization committed to implementing satisfactory corrective actions as agreed to by the OPC.

Not well-founded

There was no or insufficient evidence to conclude the institution/organization contravened the privacy legislation.

Resolved

Under the *Privacy Act*, the investigation revealed that the complaint is essentially a result of a miscommunication, misunderstanding, etc., between parties; and/or the institution agreed to take measures to rectify the problem to the satisfaction of the OPC.

Settled

The OPC helped negotiate a solution that satisfied all parties during the course of the investigation, and did not issue a finding.

Discontinued

Under the *Privacy Act*: The investigation was terminated before all the allegations were fully investigated. A case may be discontinued for various reasons, but not at the OPC's behest. For example, the complainant may no longer be interested in pursuing the matter or cannot be located to provide additional information critical to reaching a conclusion.

Under PIPEDA: The investigation was discontinued without issuing a finding. An investigation may be discontinued at the Commissioner's discretion for the reasons set out in subsection 12.2(1) of PIPEDA.

No jurisdiction

It was determined that federal privacy legislation did not apply to the institution/organization, or to the complaint's subject matter. As a result, no report is issued.

Early resolution (ER)

Applied to situations in which the issue is resolved to the satisfaction of the complainant early in the investigation process and the Office did not issue a finding.

Declined to investigate

Under PIPEDA, the Commissioner declined to commence an investigation in respect of a complaint because the Commissioner was of the view that:

- the complainant ought first to exhaust grievance or review procedures otherwise reasonably available;
- the complaint could be more appropriately dealt with by means of another procedure provided for under the laws of Canada or of a province; or,
- the complaint was not filed within a reasonable period after the day on which the subject matter of the complaint arose, as set out in subsection 12(1) of PIPEDA.

Withdrawn

Under PIPEDA, the complainant voluntarily withdrew the complaint or could no longer be practicably reached. The Commissioner does not issue a report.

Appendix 2: Statistical tables

Tables related to the *Privacy Act*

Table 1

***Privacy Act* dispositions of access and privacy complaints* by institution**

Respondent	Discontinued	No jurisdiction	Not well-founded	Resolved	Settled	Well-founded	Well-founded and resolved	Early resolved	Total
Atomic Energy of Canada Limited								1	1
Canada Border Services Agency	6		9	1	1		4	19	40
Canada Employment Insurance Commission								1	1
Canada Industrial Relations Board								1	1
Canada Post Corporation			2			2	3	23	30
Canada Revenue Agency	1		9		1	3	2	28	44
Canadian Broadcasting Corporation			3					3	6
Canadian Food Inspection Agency								1	1
Canadian Human Rights Commission							1	2	3
Canadian Radio-television and Telecommunications Commission			1					2	3
Canadian Security Intelligence Service			5	1				12	18
Canadian Transportation Agency			1					2	3
Correctional Service Canada	5		15	3	1	5	4	50	83
Crown-Indigenous Relations and Northern Affairs Canada		1	1					8	10
Defence Construction Canada			1						1
Department of Justice Canada			2				3	4	9
Elections Canada / Office of the Chief Electoral Officer			1						1

Respondent	Discontinued	No jurisdiction	Not well-founded	Resolved	Settled	Well-founded	Well-founded and resolved	Early resolved	Total
Employment and Social Development Canada	2		10	1		3		27	43
Environment and Climate Change Canada								2	2
Federal Public Service Labour Relations and Employment Board								1	1
Fisheries and Oceans Canada			6			3	2	2	13
Global Affairs Canada	1		1			1		5	8
Health Canada	1		2					7	10
Immigration, Refugees and Citizenship Canada	1		9			4	1	21	36
Indigenous Services Canada								2	2
Innovation, Science and Economic Development Canada						1		1	2
Library and Archives Canada			1					1	2
National Defence			21	1	2		5	20	49
National Energy Board			1			1		1	3
National Film Board of Canada								1	1
Office of the Correctional Investigator	2		1					1	4
Office of the Ombudsman, National Defence and Canadian Forces			1						1
Office of the Public Sector Integrity Commissioner of Canada			1						1
Office of the Superintendent of Financial Institutions Canada			1						1
Parole Board of Canada					1			1	2
Public Health Agency of Canada			2					1	3
Public Prosecution Service of Canada							1		1
Public Safety Canada								2	2
Public Service Commission of Canada			1			1		2	4
Public Services and Procurement Canada			3				1	9	13
Royal Canadian Mint								2	2

Respondent	Discontinued	No jurisdiction	Not well-founded	Resolved	Settled	Well-founded	Well-founded and resolved	Early resolved	Total
Royal Canadian Mounted Police	6		22	3	1	4	4	36	**76**
Security Intelligence Review Committee								2	**2**
Service Canada						2		1	**3**
Shared Services Canada								1	**1**
Social Sciences and Humanities Research Council of Canada			1						**1**
Statistics Canada			4					11	**15**
Status of Women Canada								2	**2**
Sustainable Development Technology Canada			2				1		**3**
Transport Canada	1		2		1		2	7	**13**
Treasury Board of Canada Secretariat			1					1	**2**
Veterans Affairs Canada	1		2	1				4	**8**
VIA Rail Canada				1		1			**2**
Total	**27**	**1**	**145**	**12**	**8**	**31**	**34**	**331**	**589**

**Privacy Act* complaints closed based on count of one for each series of complaints dealing with a related issue; excluded complaints total 223.

Table 2

Privacy Act treatment times – Early resolution cases by complaint type*

Complaint type	Count	Average treatment time (months)
Access	**175**	**3.48**
Access	167	3.32
Correction/notation	5	3.23
Language	3	12.93
Privacy	**155**	**5.29**
Accuracy	3	0.90
Collection	21	7.04
Retention and disposal	6	2.68
Use and disclosure	125	5.23
Time limits	**103**	**0.05**
Correction/notation	1	0.01
Time limits	102	0.05
Total	**433**	**3.31**

**Privacy Act* complaints closed based on count of one for each series of complaints dealing with a related issue; excluded complaints total 223.

Table 3

Privacy Act treatment times – All other investigations by complaint type*

Complaint type	Count	Average treatment time (months)
Access	**129**	**21.70**
Access	125	21.52
Correction/notation	3	22.42
Language	1	42.41
Privacy	**130**	**27.54**
Accuracy	4	14.01
Collection	31	26.57
Retention and disposal	8	24.56
Use and disclosure	87	28.78
Time limits	**674**	**6.98**
Correction/notation	1	0.75
Extension notice	10	8.78
Time limits	663	6.96
Total	**933**	**11.88**

**Privacy Act* complaints closed based on count of one for each series of complaints dealing with a related issue; excluded complaints total 223.

Table 4

Privacy Act treatment times – All closed files by disposition*

Complaint type	Number	Average treatment time (months)
Early resolved	**433**	**3.31**
All other investigations	**933**	**11.88**
Discontinued	57	12.05
No jurisdiction	1	42.66
Not well-founded	160	22.74
Resolved	14	22.45
Settled	8	31.88
Well-founded	49	20.70
Well-founded and conditionally resolved	67	5.73
Well-founded and resolved	577	8.23
Total	**1,366**	**9.16**

**Privacy Act* complaints closed based on count of one for each series of complaints dealing with a related issue; excluded complaints total 223.

Table 5

Privacy Act breaches by institution

Respondent	Count
Bank of Canada	1
Canada Border Services Agency	2
Canada Post Corporation	2
Canada Revenue Agency	6
Canadian Broadcasting Corporation	1
Canadian Heritage	2
Communications Security Establishment Canada	1
Correctional Service Canada	10
Crown-Indigenous Relations and Northern Affairs Canada	1
Department of Finance Canada	1
Employment and Social Development Canada	78
Environment and Climate Change Canada	1
Fisheries and Oceans Canada	1
Global Affairs Canada	2
Immigration, Refugees and Citizenship Canada	6
Innovation, Science and Economic Development Canada	1
National Energy Board	1
Natural Resources Canada	1
Non-Public Property and Staff of the Non-Public Funds, Canadian Forces	1
Office of the Correctional Investigator	3
Office of the Information Commissioner of Canada	1
Public Prosecution Service of Canada	1
Public Safety Canada	1
Public Service Commission of Canada	4
Public Services and Procurement Canada	4
Royal Canadian Mounted Police	11
Shared Services Canada	3
Statistics Canada	6
Status of Women Canada	1
Total	**155**

Table 6

Privacy Act complaints and breaches

Category	Total
Accepted	
Privacy	230
Access	391
Time limits	799
Total accepted*	**1,420**
Closed through early resolution	
Access	155
Privacy	175
Time limits	103
Total	**433**
Closed through all other investigations	
Access	129
Privacy	130
Time limits	674
Total	**933**
Total closed **	**1,366**
Breaches received	
Accidental disclosure	61
Loss	69
Theft	8
Unauthorized access	17
Total received	**155**

*Includes one representative complaint for each of several series of related complaints and complaints submitted by a small number of individual complainants; excluded complaints total 95.

***Privacy Act* complaints closed based on one of each series of complaints dealing with a related issue; excluded complaints total 223.

Table 7

Privacy Act complaints accepted by complaint type

Complaint type	Early resolution		Investigation		Total number	Total percentage*
	Number	Percentage*	Number	Percentage*		
Privacy						
Accuracy	4	1%	1	0%	5	0%
Collection	29	5%	23	3%	52	4%
Retention and disposal	10	2%	2	0%	12	1%
Use and disclosure	133	24%	28	3%	161	11%
Access						
Access	250	46%	116	13%	366	26%
Correction/notation	18	3%	6	1%	24	2%
Language	1	0%			1	0%
Time limits						
Correction/notation	1	0%	1	0%	2	0%
Extension notice			12	1%	12	1%
Time limits	102	19%	683	78%	785	55%
Total	**548**	**100%**	**872**	**100%**	**1,420**	**100%**

* Figures may not sum to total due to rounding.

Table 8

Privacy Act top 10 institutions by complaints accepted*

	Privacy		Access		Time limits		Total
Respondent	Early resolution	Investigation	Early resolution	Investigation	Early resolution	Investigation	
Correctional Service Canada	20	4	31	14	11	346	426
Royal Canadian Mounted Police	23	6	27	13	14	190	273
National Defence	13	6	25	6	18	53	121
Canada Border Services Agency	13	7	31	23	6	29	109
Canada Revenue Agency	21	4	19	12	6	17	79
Immigration, Refugees and Citizenship Canada	11	1	18	1	22	6	59
Employment and Social Development Canada	13	1	15	6	2	2	39
Statistics Canada	4	10	7	1		12	34
Canada Post Corporation	10	1	13	1	2	2	29
Public Services and Procurement Canada	5	1	9		7	5	27
Total	**133**	**41**	**195**	**77**	**88**	**662**	**1,196**

*Includes one representative complaint for each of several series of related complaints and complaints submitted by a small number of individual complainants; excluded complaints total 95.

Table 9

Privacy Act top 10 institutions in 2018-19 by complaints accepted* and fiscal year

Respondent	2015-16	2016-17	2017-18	2018-19
Correctional Service Canada	547	389	440	426
Royal Canadian Mounted Police	120	160	232	273
National Defence	77	146	93	121
Canada Border Services Agency	88	107	76	109
Canada Revenue Agency	85	65	63	79
Immigration, Refugees and Citizenship	44	60	29	59
Employment and Social Development Canada	42	36	24	39
Statistics Canada	5	22	4	34
Canada Post Corporation	17	19	33	29
Public Services and Procurement Canada	10	25	49	27
Total	**1,035**	**1,029**	**1,043**	**1,196**

*Includes one representative complaint for each of several series of related complaints and complaints submitted by a small number of individual complainants; excluded complaints total 95.

Table 10

Privacy Act complaints accepted* by institution

Respondent	Early resolution	Investigation	Total
Administrative Tribunals Support Service of Canada	1	2	**3**
Atomic Energy of Canada Limited	1	2	**3**
Bank of Canada	1		**1**
Canada Border Services Agency	50	59	**109**
Canada Council for the Arts	1		**1**
Canada Employment Insurance Commission	1		**1**
Canada Industrial Relations Board	1		**1**
Canada Post Corporation	25	4	**29**
Canada Revenue Agency	46	33	**79**
Canada School of Public Service		2	**2**
Canadian Broadcasting Corporation	2		**2**
Canadian Food Inspection Agency	1	1	**2**
Canadian Human Rights Commission		1	**1**
Canadian Institutes of Health Research	1		**1**
Canadian Northern Economic Development Agency		1	**1**
Canadian Radio-television and Telecommunications Commission	2		**2**
Canadian Security Intelligence Service	19	5	**24**
Canadian Transportation Agency	1		**1**
Citizenship and Immigration Canada	1		**1**
Civilian Review and Complaints Commission for the Royal Canadian Mounted Police		6	**6**
Communications Security Establishment Canada	1	2	**3**
Correctional Service Canada	62	364	**426**

Respondent	Early resolution	Investigation	Total
Crown-Indigenous Relations and Northern Affairs Canada	9	1	10
Department of Justice Canada	5	11	16
Employment and Social Development Canada	30	9	39
Environment and Climate Change Canada	4		4
Federal Public Service Labour Relations and Employment Board	1		1
Fisheries and Oceans Canada	5	3	8
Global Affairs Canada	9	11	20
Health Canada	5	1	6
Immigration and Refugee Board of Canada	3		3
Immigration, Refugees and Citizenship Canada	51	8	59
Indigenous Services Canada	2	1	3
Innovation, Science and Economic Development Canada	1	1	2
Library and Archives Canada	1		1
National Defence	56	65	121
National Energy Board		1	1
Natural Sciences and Engineering Research Council of Canada	4	1	5
Non-Public Property and Staff of the Non-Public Funds, Canadian Forces	1		1
Office of the Correctional Investigator	1	4	5
Office of the Ombudsman, National Defence and Canadian Forces		1	1
Parks Canada Agency	1	1	2
Parole Board of Canada	2	4	6
Public Health Agency of Canada	1		1
Public Prosecution Service of Canada		2	2
Public Safety Canada	1	14	15
Public Service Commission of Canada	4	1	5
Public Services and Procurement Canada	21	6	27
Royal Canadian Mint	2		2
Royal Canadian Mounted Police	64	209	273
Security Intelligence Review Committee	2	2	4
Service Canada	1		1
Shared Services Canada	1		1
Social Sciences and Humanities Research Council of Canada	4	3	7
Statistics Canada	11	23	34
Transport Canada	10	2	12
Treasury Board of Canada Secretariat	2	1	3
Veterans Affairs Canada	16	4	20
Total	**548**	**872**	**1,420**

*Includes one representative complaint for each of several series of related complaints and complaints submitted by a small number of individual complainants; excluded complaints total 95.

Table 11

Privacy Act complaints accepted by province, territory or other

	Early resolution		Investigation		Total number	Total percentage*
Province, territory or other	Number	Percentage*	Number	Percentage*		
Ontario	215	39.23%	359	41.17%	574	40.42%
Quebec	107	19.53%	105	12.04%	212	14.93%
Nova Scotia	11	2.01%	17	1.95%	28	1.97%
New Brunswick	9	1.64%	11	1.26%	20	1.41%
Manitoba	17	3.10%	16	1.83%	33	2.32%
British Columbia	101	18.43%	211	24.20%	312	21.97%
Prince Edward Island	0	0.00%	2	0.23%	2	0.14%
Saskatchewan	18	3.28%	16	1.83%	34	2.39%
Alberta	44	8.03%	111	12.73%	155	10.92%
Newfoundland and Labrador	7	1.28%	13	1.49%	20	1.41%
Northwest Territories	2	0.36%	0	0.00%	2	0.14%
Yukon	1	0.18%	0	0.00%	1	0.07%
Nunavut	0	0.00%	0	0.00%	0	0.00%
US	2	0.36%	8	0.92%	10	0.70%
Other (non US)	3	0.55%	1	0.11%	4	0.28%
Not specified	11	2.01%	2	0.23%	13	0.92%
Total	**548**	**100.00%**	**872**	**100.00%**	**1,420**	**100.00%**

* Figures may not sum to total due to rounding.

Table 12

Privacy Act dispositions by complaint type*

Complaint type	Discontinued	No jurisdiction	Not well-founded	Resolved	Settled	Well-founded	Well-founded and conditionally resolved	Well-founded and resolved	Early resolved	Total
Access										
Access	7		73	7	3	4		30	168	292
Correction/notation			2	1					5	8
Language				1					3	4
Privacy										
Accuracy	1		1	1		1			3	7
Collection	9		14		2	6			21	52
Retention and disposal	1		6			1			6	14
Use and disclosure	9	1	49	2	3	19		4	125	212
Time limits										
Correction/notation								1	1	2
Extension notice	1		3			4		2		10
Time limits	29		12	1		14	67	540	102	765
Total	**57**	**1**	**160**	**13**	**8**	**49**	**67**	**577**	**434**	**1,366**

**Privacy Act* complaints closed based on one of each series of complaints dealing with a related issue; excluded complaints total 223.

Table 13

Privacy Act dispositions of time limits by institution*

Respondent	Discontinued	Not well-founded	Resolved	Well-founded	Well-founded and conditionally resolved	Well-founded and resolved	Early resolved	Total
Canada Border Services Agency					1	17	6	24
Canada Post Corporation		2		2		1	2	7
Canada Revenue Agency	1					12	6	19
Canadian Security Intelligence Service		1				2	1	4
Civilian Review and Complaints Commission for the Royal Canadian Mounted Police						1		1
Correctional Service Canada	9	1		12	66	272	11	371
Crown-Indigenous Relations and Northern Affairs Canada							1	1
Department of Justice Canada						3		3
Employment and Social Development Canada						3	2	5
Global Affairs Canada						1	2	3
Health Canada				2		1		3
Immigration, Refugees and Citizenship Canada	1					7	22	30
National Defence	2		1			57	18	78
Office of the Correctional Investigator		1						1
Public Prosecution Service of Canada						1		1
Public Service Commission of Canada		1						1
Public Services and Procurement Canada				1		6	7	14
Royal Canadian Mounted Police	5	7		1		152	14	179
Security Intelligence Review Committee						1		1
Social Sciences and Humanities Research Council of Canada		2						2
Statistics Canada	12							12
Transport Canada						5	3	8
Treasury Board of Canada Secretariat							1	1
Veterans Affairs Canada						1	7	8
Total	**30**	**15**	**1**	**18**	**67**	**543**	**103**	**777**

**Privacy Act* complaints closed based on one of each series of complaints dealing with a related issue; excluded complaints total 223.

Tables related to PIPEDA

Table 1

PIPEDA complaints accepted* by industry sector

Industry sector	Number	Percentage of all complaints accepted **
Accommodations	36	9%
Construction	5	1%
Entertainment	4	1%
Financial	75	20%
Food and beverage	5	1%
Government	1	0%
Health	2	1%
Individual	1	0%
Insurance	17	4%
Internet	37	10%
Manufacturing	18	5%
Non-profit organizations	3	1%
Professionals	11	3%
Publishing (except internet)	4	1%
Rental	2	1%
Sales/Retail	29	8%
Services	41	11%
Telecommunications	48	13%
Transportation	37	10%
Utilities	3	1%
Not specified	1	0%
Total	**380**	**100%**

* Figures may not sum to total due to rounding.

** PIPEDA complaints accepted based on count of one for each series of complaints dealing with a related issue; excluded complaints total 100.

Table 2

PIPEDA complaints accepted* by complaint type

Complaint type	Number	Percentage of all complaints accepted**
Access	110	29%
Accountability	8	2%
Accuracy	3	1%
Appropriate purposes	3	1%
Challenging compliance	1	0%
Collection	49	13%
Consent	64	17%
Correction/notation	2	1%
Identifying purposes	1	0%
Other	1	0%
Retention	10	3%
Safeguards	59	16%
Use and disclosure	69	18%
Total	**380**	**100%**

* PIPEDA complaints accepted based on count of one for each series of complaints dealing with a related issue; excluded complaints total 100.

** Figures may not sum to total due to rounding.

Table 3

PIPEDA investigations closed* by industry sector and disposition

Sector category	Early resolved	Declined	Discontinued (under 12.2)	No jurisdiction	Not well-founded	Settled	Well-founded	Well-founded and conditionally resolved	Well-founded and resolved	Withdrawn	Total
Accommodations	13		1		1		1		2		18
Construction	1										1
Entertainment	4							1			5
Financial	27		10		3		2	3	6	5	56
Food and beverage	3									1	4
Government	1										1
Health			8	2						1	11
Insurance	6	1	1	1	3				3		15
Internet	24		3		1	1		1	2	4	36
Manufacturing	4								1		5
Non-profit organizations			1								1
Professionals	7		1	2	2		1		1		14
Publishing (except Internet)	4							2			6

Sector category	Early resolved	Declined	Discontinued (under 12.2)	No jurisdiction	Not well-founded	Settled	Well-founded	Well-founded and conditionally resolved	Well-founded and resolved	Withdrawn	Total
Rental	1										1
Sales/Retail	17		1						2	1	21
Services	22			1		1		1	1		26
Telecommunications	31		2		1			2	1	2	39
Transportation	11		4						2	1	18
Utilities	1		1								2
Not specified	1						1				2
Total	178	1	33	6	11	2	5	10	21	15	282

*PIPEDA complaints accepted based on count of one for each series of complaints dealing with a related issue; excluded complaints total 110.

Table 4

PIPEDA investigations closed* by complaint type and disposition

Complaint type	Early resolved	Declined to investigate	Discontinued (under 12.2)	No jurisdiction	Not well-founded	Settled	Well-founded	Well-founded and conditionally resolved	Well-founded and resolved	Withdrawn	Total
Access	46		13	3	2		1	3	12	4	84
Accountability	2		2		1						5
Accuracy	2		1		1						4
Appropriate purposes	1		1								2
Collection	26				1	1		2	2	2	34
Consent	32	1	7	1	3	1	2	4		8	59
Correction/ notation	2									1	3
Identifying purposes					1						1
Retention	8										8
Safeguards	16		4		1				3		24
Use and disclosure	43		5	2	1		2	1	3		57
Other									1		1
Total	178	1	33	6	11	2	5	10	21	15	282

*PIPEDA complaints accepted based on count of one for each series of complaints dealing with a related issue; excluded complaints total 110.

Table 5

PIPEDA investigations* – Average treatment time by disposition

Disposition	Count	Average treatment time in months
Early resolved	178	2.7
Declined to investigate	1	6.7
Discontinued (under 12.2)	33	9.5
No jurisdiction	6	10.8
Not well-founded	11	16.8
Settled	2	14.6
Well-founded	5	20.3
Well-founded and conditionally resolved	10	22.4
Well-founded and resolved	21	15.9
Withdrawn	15	20.2
Total	**282**	
Overall weighted average		**7.3**

*PIPEDA investigations based on count of one for each series of complaints dealing with a related issue; excluded complaints total 110.

Table 6

PIPEDA investigations* – Average treatment times by complaint and disposition types

	Early resolved		Dispositions not early resolved		All dispositions	
Complaint type	**Number**	**Average treatment time in months**	**Number**	**Average treatment time in months**	**Number**	**Average treatment in months**
Access	46	3.1	38	14.3	84	8.2
Accountability	2	2.6	3	3.1	5	2.9
Accuracy	2	4.0	2	19.6	4	11.8
Appropriate purposes	1	2.0	1	17.6	2	9.8
Collection	26	2.0	8	22.3	34	6.8
Consent	32	2.8	27	16.6	59	9.1
Correction/notation	2	0.9	1	15.3	3	5.7
Identifying purposes			1	10.2	1	10.2
Retention	8	2.3			8	2.3
Safeguards	16	2.4	8	20.6	24	8.4
Use and disclosure	43	3.0	14	8.7	57	4.4
Other			1	14.6	1	14.6
Total	**178**	**2.7**	**104**	**15.0**	**282**	**7.3**

*PIPEDA investigations based on count of one for each series of complaints dealing with a related issue; excluded complaints total 110.

Table 7

PIPEDA breach notifications by industry sector and incident type

Sector	Incident type					Percentage of total incidents*
	Accidental disclosure	Loss	Theft	Unauthorized access	Total incidents per sector	
Accommodations				5	5	2%
Construction	2				2	1%
Entertainment			1	3	4	1%
Financial	20	3	9	38	70	22%
Food and beverage		1			1	0%
Government	1		1	1	3	1%
Health	7	1	1	3	12	4%
Insurance	12	1	6	5	24	8%
Internet	5		1	8	14	4%
Manufacturing	2			10	12	4%
Mining and oil and gas extraction	1			1	2	1%
Non-profit organizations	8	1	1	4	14	4%
Professionals	3	1	2	6	12	4%
Publishing	1		1	6	8	3%
Sales/Retail	11	19	1	26	57	18%
Services	2			15	17	5%
Telecommunications	6		3	43	52	17%
Transportation	1			3	4	1%
Utilities				1	1	0%
Not specified	1				1	0%
Total	**83**	**27**	**27**	**178**	**315**	**100%**

* Figures may not sum to total due to rounding.

Appendix 3: Investigation process

PRIVACY ACT INVESTIGATION PROCESS

Intake

Individuals make written submissions to our Office about alleged violations of the *Privacy Act*. Our Intake Unit reviews the matter to determine whether it constitutes a complaint, i.e., whether the allegations could constitute a contravention of the Act, and the most efficient manner in which to resolve it.

An individual may complain about any matter specified in section 29 of the *Privacy Act*, for example:

- denial of access or unacceptable delay in providing access to his or her personal information held by an institution;
- improper collection, use or disclosure of personal information, or
- inaccuracies in personal information used or disclosed by an institution.

It is sometimes possible to immediately address issues, eliminating the need for our Office to pursue the matter as a standard investigation. In these cases, we simply resolve the matter through early resolution. The Privacy Commissioner may also initiate a complaint if satisfied there are reasonable grounds to investigate a matter.

Complaint

No

The individual is advised, for example, that the matter is not in our jurisdiction.

Yes

An investigator is assigned to the case.

Early resolution

A complaint may be resolved before a standard investigation is undertaken if, for example, the issue has already been fully dealt with in another investigation and the institution has ceased the practice or the practice does not contravene the Act.

Standard investigation

The investigation provides the factual basis for the Commissioner to determine whether the individual's rights under the *Privacy Act* have been contravened.

The investigator writes to the institution, outlining the substance of the complaint. The investigator gathers the facts related to the complaint through representations from both parties and through independent inquiry, interviews of witnesses, and review of documentation.

Through the Commissioner or his delegate, the investigator has the authority to receive evidence, enter premises where appropriate, and examine or obtain copies of records found on any premises.

Discontinued

A complaint may be discontinued if, for example, a complainant decides not to pursue it, or a complainant cannot be located.

Analysis (on next page)

Settled (on next page)

Note: a broken line (- - - -) indicates a *possible* outcome.

Standard investigation

(continued from previous page)

Analysis

The investigator analyzes the facts and prepares recommendations to the Commissioner or his delegate. The investigator will contact the parties as necessary and review the facts gathered during the course of the investigation. The investigator may also tell the parties what he or she will be recommending, based on the facts, to the Commissioner or his delegate. At this point, the parties may make further representations.

Analysis will include internal consultations with various directorates, for example, Legal Services, Policy, Research and Parliamentary Affairs, and Technology Analysis, as appropriate.

Settled

The OPC seeks to resolve complaints and to prevent contraventions from recurring. The Commissioner encourages resolution through negotiation and persuasion. The investigator assists in this process.

Findings

The Commissioner or his delegate reviews the file and assesses the report. The Commissioner or his delegate, not the investigator, decides what the appropriate outcome should be and whether recommendations to the institution are warranted.

The Commissioner or his delegate sends letters of findings to the parties. The letters outline the basis of the complaint, the relevant findings of fact, the analysis, and any recommendations to the institution. The Commissioner or his delegate may ask the institution to respond in writing, within a particular timeframe, outlining its plans for implementing any recommendations.

The possible findings are:

Not well-founded: The evidence, on balance, does not lead the Commissioner or his delegate to conclude that the complainant's rights under the Act have been contravened.

Well-founded: The institution failed to respect a provision of the Act.

Well-founded, resolved: The investigation substantiated the allegations and the institution has agreed to take corrective measures to rectify the problem.

Resolved: The evidence gathered in the investigation supports the allegations raised in the complaint, but the institution has agreed to take corrective measures to rectify the problem, to the satisfaction of this Office. The finding is used for those complaints in which "well-founded" would be too harsh to fit what essentially is a miscommunication or misunderstanding.

In the letter of findings, the Commissioner or his delegate informs the complainant of his or her rights of recourse to the Federal Court on matters of denial of access to personal information.

Where recommendations have been made to an institution, OPC staff will follow up to verify that they have been implemented.

The complainant or the Commissioner may choose to apply to the Federal Court for a hearing of the denial of access. The Federal Court has the power to review the matter and determine whether the institution must provide the information to the requester.

Note: a broken line (- - - -) indicates a *possible* outcome.

PIPEDA INVESTIGATION PROCESS

Intake

Individuals make written complaints to the OPC about violations of the Act. Our Intake Unit reviews these complaints, and, if necessary, follows up with complainants to seek clarification and gather additional information.

If complainants have not raised their concerns directly with the organization, we will ask them to do so in order to try to resolve the issue and then to come back to us if they are unsuccessful.

The Intake Unit is also sometimes able to immediately address issues. For example, if we have previously investigated the type of issue being raised and have determined that the activities are compliant with PIPEDA, an intake officer will explain this to the individual. Or, if we have previously determined that we do not have jurisdiction over the organization or type of activity, an intake officer will explain this and, where appropriate, refer the individual to other resources or sources of assistance.

In cases where the Intake Unit is not able to immediately address issues (and once the necessary information is gathered), the matter is accepted by our Office as a formal complaint. The Privacy Commissioner may also initiate a complaint if satisfied there are reasonable grounds to investigate a matter.

Complaint declined

The Commissioner may decide to decline to investigate a complaint if certain conditions under subsection 12(1) of the Act are met. The complainant may request that the Commissioner reconsider this decision.

Sent to investigation

Complaints of a serious, systemic or otherwise complex nature, for example, uncertain jurisdictional matters, multiple allegations or complex technical issues, are assigned to an investigator.

Sent to early resolution officer

Complaints which we believe could potentially be resolved quickly are sent to an early resolution officer. These complaints include matters where our Office has already made findings on the issues; where the organization has already dealt with the allegations to our satisfaction; or where it seems possible that allegations can be easily remedied.

Investigation

Investigations provide the factual basis for the Commissioner to determine whether the individual's rights have been contravened under PIPEDA.

The investigator writes to the organization, outlining the substance of the complaint. The investigator gathers the facts related to the complaint through representations from both parties and through independent inquiry, interviews of witnesses, and review of documentation. Through the Commissioner or his delegate, the investigator has the authority to receive evidence, enter premises where appropriate, and examine or obtain copies of records found on any premises.

Transferred to investigation

If early resolution is unsuccessful, the case is transferred to an investigator.

Early resolution

Early resolution officers encourage resolutions through mediation, negotiation and persuasion.

Discontinued

A complaint may be discontinued if, for example, a complainant decides not to pursue it or cannot be located, or if certain conditions, described in section 12.2 of the Act, are met.

Analysis (on next page)

Settled (on next page)

Standard investigation

(continued from previous page)

Analysis

The investigator analyses the facts and prepares recommendations to the Commissioner or his delegate.

The investigator will contact the parties and review the facts gathered during the course of the investigation. The investigator will also advise the parties of his or her recommendations, based on the facts, to the Commissioner or his delegate. At this point, the parties may make further representations.

Analysis will include internal consultations with various directorates, for example, Legal Services, Policy, Research and Parliamentary Affairs, and Technology Analysis, as appropriate.

Settled

The OPC seeks to resolve complaints and to prevent contraventions from recurring. The OPC helps negotiate a solution that satisfies all involved parties during the course of the investigation. The investigator assists in this process.

No jurisdiction

The OPC determines that PIPEDA does not apply to the organization or activities being complained about.

Findings

The Commissioner or his delegate reviews the file and assesses the report. The Commissioner or his delegate (not the investigator) decides what the appropriate outcome should be and whether recommendations to the organization are warranted.

Preliminary report

If the results of the investigation indicate that there likely has been a contravention of PIPEDA, the Commissioner or his delegate recommends to the organization how to remedy the matter, and asks the organization to indicate within a set time period how it will implement the recommendation.

Final report and letters of findings

The Commissioner or his delegate sends letters of findings to the parties. The letters outline the basis of the complaint, the relevant findings of fact, the analysis, and the response of the organization to any recommendations made in the preliminary report.

(The possible findings are described in Appendix 1 – Definitions.)

In the letter of findings, the Commissioner or his delegate informs the complainant of his or her rights of recourse to the Federal Court.

Where recommendations have been made to an organization but have not yet been implemented, the OPC will ask the organization to keep us informed, on a predetermined schedule after the investigation, so that we can assess whether corrective action has been taken.

The complainant or the Commissioner may choose to apply to the Federal Court for a hearing of the matter. The Federal Court has the power to order the organization to correct its practices. The Court can award damages to a complainant, including damages for humiliation. There is no ceiling on the amount of damages.

Appendix 4: Substantially similar legislation

Subsection 25(1) of PIPEDA requires our Office to report annually to Parliament on the "extent to which the provinces have enacted legislation that is substantially similar" to the Act.

Under paragraph 26(2)(b) of PIPEDA, the Governor in Council may issue an Order exempting an organization, a class of organizations, an activity or a class of activities from the application of PIPEDA with respect to the collection, use or disclosure of personal information that occurs within a province that has passed legislation that is "substantially similar" to PIPEDA.

On August 3, 2002, Industry Canada (now known as Innovation, Science and Economic Development Canada) published the Process for the Determination of "Substantially Similar" Provincial Legislation by the Governor in Council, outlining the policy and criteria used to determine whether provincial legislation will be considered substantially similar. Under the policy, laws that are substantially similar:

- provide privacy protection that is consistent with and equivalent to that in PIPEDA;
- incorporate the 10 principles in Schedule 1 of PIPEDA;
- provide for an independent and effective oversight and redress mechanism with powers to investigate; and
- restrict the collection, use and disclosure of personal information to purposes that are appropriate or legitimate.

Organizations that are subject to provincial legislation deemed substantially similar are exempt from PIPEDA with respect to the collection, use or disclosure of personal information occurring within the respective province. Accordingly, PIPEDA continues to apply to the collection, use or disclosure of personal information in connection with the operations of a federal work, undertaking or business in the respective province, as well as to the collection, use or disclosure of personal information outside the province.

The following provincial laws that have been declared substantially similar to PIPEDA:

- Quebec's *An Act Respecting the Protection of Personal Information in the Private Sector*;
- British Columbia's *Personal Information Protection Act*;
- Alberta's *Personal Information Protection Act*;
- Ontario's *Personal Health Information Protection Act*, with respect to health information custodians;
- New Brunswick's *Personal Health Information Privacy and Access Act*, with respect to health information custodians;
- Newfoundland and Labrador's *Personal Health Information Act*, with respect to health information custodians; and
- Nova Scotia's *Personal Health Information Act*, with respect to health information custodians.

Appendix 5: Report of the Privacy Commissioner, Ad Hoc

The Privacy Commissioner, Ad Hoc investigates complaints about how the Office of the Privacy Commissioner handles requests it receives for access to personal information. This role was created because the Office cannot investigate itself on such matters.

I became Privacy Commissioner, Ad Hoc in April 2018, and as such, I have all the same powers as the Commissioner with regard to investigations and may issue recommendations on how to resolve complaints I receive. I came to this role having been New Brunswick's Access to Information and Privacy Commissioner from 2010 to 2017. I was also interim Conflict of Interest Commissioner for New Brunswick for one year (2015–16). Prior to that, I was a lawyer in general practice for 24 years, appearing before all levels of the courts, including the Supreme Court of Canada.

In 2018-2019, there was one complaint involving the Office of the Privacy Commissioner, which resulted in a finding that while the requester (complainant) had received access to all personal information to which she was entitled, the case highlighted the fact that better explanations could have been provided to the requester at the outset. No need to issue a recommendation in that case. Another matter was examined in depth but revealed no basis to be received as a proper complaint. The rest of the work I received consisted of correspondence from individuals who were not satisfied with the Office's handling of their cases, but which subject matters fell outside of my authority to act. I sent letters to those individuals with those explanations.

Anne E. Bertrand, Q.C.
Privacy Commissioner, Ad Hoc