Office of the
Privacy Commissioner
of Canada

THE CASE FOR REFORMING THE *PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT*

May 2013

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The environment in which personal information is collected, used and disclosed has undergone a dramatic reshaping since the *Personal Information Protection and Electronic Documents Act* (PIPEDA) was passed at the turn of the 21st century.

In that short period, the advances in computing power and storage, and the massive expansion in the scale of personal information that organizations can collect and store, use and disclose about individuals have combined to pave the way for an explosion in the role that personal information plays in the digital economy. With those changes have come risks that individuals' information is used in ways that may be intrusive, or that individuals do not anticipate or knowingly choose, as organizations rush to create new services and products. In some cases, their personal information is at risk of being stolen or lost because of lapses in appropriate security measures.

Incentives are needed to ensure that organizations are building privacy protections into their products and services from the start. A stronger enforcement regime is one such incentive. Other incentives include more robust accountability and transparency to ensure that Canadians' personal information is appropriately protected in a complex, globally connected environment.

Such measures will address current and future privacy challenges; improve Canadians' trust in the digital economy; reinforce Canadian innovation and growth; and ensure that Canada remains a country with an appropriate, up-to-date and balanced privacy framework.

This paper recommends the following changes to PIPEDA to build such incentives:

- Reform PIPEDA to provide for stronger enforcement powers. These could include statutory damages (administered by the Federal Court); or giving the Commissioner the power to make orders; or affording the Commissioner with the power to impose administrative monetary penalties; or a combination of the above;
- Require organizations to report breaches of personal information to the Commissioner and to notify affected individuals, where warranted, so that appropriate mitigating measures can be taken in a timely manner;
- Require organizations to publicly report on the number of disclosures they make to law enforcement under paragraph 7(3)(c.1), without knowledge or consent, and without judicial warrant, in order to shed light on the frequency and use of this extraordinary exception; and
- Modify the accountability principle in Schedule 1 to include a requirement for organizations to demonstrate accountability upon request; to incorporate the concept of "enforceable agreements"; and to make certain accountability provisions subject to review by the Federal Court.

PIPEDA is technology-neutral and principles-based – two qualities that should remain as these are strengths of the law. With the recommended changes, PIPEDA can evolve into a more modern personal information protection law that mirrors improvements and strengths of other data protection laws in Canada and internationally, thereby ensuring that Canadians' personal information is protected in the digital economy.

INTRODUCTION

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) received Royal Assent on April 13, 2000, and came into force in stages, beginning on January 1, 2001. PIPEDA came fully into force on January 1, 2004.

PIPEDA was "enacted to alleviate consumer concerns about privacy and to allow Canada's business community to compete in the global digital economy.[1] The policy goal was to build trust in electronic commerce.[2]

The legislation applies to organizations that collect, use or disclose personal information in the course of commercial activities. It also applies to the collection, use and disclosure of personal information pertaining to the employees of federal works, undertakings and businesses (FWUBs) – banks, airlines, telecommunications and broadcasting companies and other federally regulated industries.[3]

PIPEDA contains a provision requiring a review of the legislation every five years to ensure that the legislation is operating as it should, with the desired effects. The first review began in 2006, and resulted in recommendations from the Standing Committee on Access to Information, Privacy and Ethics (ETHI) to the Government. The Government responded to the Committee by introducing legislation in 2010, which died on the Order Paper nearly one year later when an election was called. It was later re-introduced as Bill C-12 in the fall of 2011, which, as of the date of this publication, has not passed Second Reading. The second review of PIPEDA is also now overdue.

In 2012, the ETHI Committee studied privacy and social media. On April 23, 2013, the Committee issued its report, which included seven recommendations and asked for a government response. Appended to the report was dissenting report issued by the New Democratic Party (NDP), which included nine recommendations. The study provided an important opportunity to examine many of the emerging privacy issues related to new technology[4].

Over the years, the Office of the Privacy Commissioner of Canada (OPC) has undertaken a number of studies and consultations to better understand the challenges of the current environment and to gauge the effectiveness of the legislation. We also have more than a decade of practical, hands-on experience in investigating complaints, conducting audits, and monitoring breaches of personal information – at least the few that are brought to our attention on a voluntary basis or through media reports.

This position paper outlines our observations on how the environment has changed since the turn of the 21st century, and details some of the most significant pressure points that make or will make it difficult to enforce PIPEDA and ensure that organizations are complying with the law. The paper also offers our views on how the Act could be improved to encourage proactive compliance with the law.

CHALLENGES TO PERSONAL INFORMATION PROTECTION IN THE DIGITAL ECONOMY

The environment in which personal information is collected, used and disclosed has undergone a dramatic reshaping since PIPEDA came into existence. In 2001, there were almost no social networking sites, no video sharing sites, and no microblogging. Cell phones were becoming more prevalent, but were not ubiquitous, nor were they used to surf the web, play games, or reveal location. In the early part of the decade, the Web was growing and some business was online, but not to the degree that we now see. Even since the last review in 2006, advances in computing power and storage, and the massive expansion in the scale of personal information that organizations can collect and store, use and disclose about individuals, have combined to pave the way for an explosion in the role that personal information plays in the digital economy.

Technology is changing quickly and the online world has been reshaped thanks to the new ways in which individuals can communicate and share personal information. However, the large-scale adoption and use of various social media sites by organizations and individuals is blurring the lines between commercial and non-commercial activities and private and public lives. And the consequences are starting to become clear.

Big data and data giants

Many people live much of their lives online. According to some estimates, Canadians lead the world in Internet use, averaging 43.5 hours a month, twice the world average.[5]

When we browse online, conduct searches, communicate with our friends or download music, we create data trails that reveal a great deal about who we are – our interests, our habits, our opinions – and in many cases even where we are.

We now live in what is being called the era of "big data". According to IBM, we are globally creating 2.5 quintillion bytes daily (which is approximately equivalent to 57.5 billion 32 GB iPads[6]). Ninety per cent of the data that exists in the world today has been created in the last two years.[7]

Personal information is central to the global digital economy. Some organizations that amass vast amounts of Canadians' personal information have grown into data giants, quasi-monopolies that have the ability to glean deep insight into the interests, habits and opinions of individual Internet users. Some of the largest companies boast customers or users in the hundreds of millions. Facebook, for example, has more than one billion users worldwide, including almost 20 million users in Canada. Twitter currently has over 500 million users. Even smaller organizations, particularly those with a digital presence, are increasingly collecting large quantities of personal information[8].

Most Internet companies offer their services at no monetary cost. They are, however, under increasing pressure to find ways to turn a profit from their services, with one of the most obvious options being to capitalize upon their treasure trove of personal information. It is a highly competitive environment, with new players appearing seemingly daily. Individuals' personal habits and details are tracked, profiled and targeted in the rush to innovate, improve services and find new markets. Increasingly, many companies are seeking to combine online and offline

data, which will give them more insight into their customers and enable them to anticipate their needs and wants – sometimes even before individuals are aware of them[9].

At the same time, individuals' trust has also been threatened – trust that is needed for the digital economy to thrive. Seventy percent of Canadians we surveyed in 2012 believe that they have less personal information protection than they did 10 years ago. Fifty-six percent say they are not confident that they know how new technologies affect their privacy, up from forty-seven percent in 2000[10]. As the ETHI Committee noted, social media is a rapidly evolving industry, "one that both experiments with the boundaries of privacy and needs privacy to ensure consumers' trust[11]." We would argue that this is true of all players in the digital economy.

As the environment evolves, the risks to privacy continue to grow. Organizations are using personal information in ways previously unimaginable. While many of these new uses will have the potential to benefit individuals and society, there are risks that personal information may be used in ways that are highly intrusive and offend our sense of privacy. Even when the information is not misused, it could be lost, accessed without authorization or stolen by sophisticated hackers.

Given that the goal of PIPEDA is to achieve a balance between the privacy rights of individuals and the legitimate needs of organizations to collect, use or disclose personal information for an appropriate purpose, it is important to examine whether that objective is being met in the evolving environment and how PIPEDA could be improved to better achieve that goal.

PRESSURE POINTS: CHALLENGES IN ENFORCING PIPEDA AND RECOMMENDATIONS TO ENSURE COMPLIANCE

There are four pressure points that we have identified in the 12 years in which we have been overseeing compliance with PIPEDA and monitoring the changing environment. They largely concern PIPEDA's current enforcement model given an evolving international context and our ability to hold organizations to account for, and be transparent about, their personal information handling practices

Pressure Point 1: Enforcement

Under the Act, the Privacy Commissioner of Canada is an "administrative investigator[12]," with a range of powers, including the ability to initiate her own investigations and audits (with reasonable grounds), and the power to compel evidence and enter premises when conducting investigations. The Commissioner may seek resolution through negotiation, persuasion and mediation. While the Commissioner may encourage compliance by naming respondent organizations when it is deemed in the public interest, she herself has no direct enforcement powers. The Commissioner can only, in certain circumstances, apply to the Federal Court to have the Court hear certain matters raised in complaints to her Office; order the respondent to take action to correct its practices; or award damages to the complainant.

The appropriateness of the current PIPEDA enforcement model has been the subject of debate prior to the law coming into force and in the ensuing years. While the question was raised during the first mandated review of the law in 2006, the Privacy Commissioner opted not to propose changes to the enforcement structure at that time for a number of reasons. The Office was just emerging from a period of instability, scrutiny and reduced capacity, and it was still early days in terms of interpreting and applying PIPEDA. Instead, the Office signaled its intent to make greater use of its existing powers to conduct audits, initiate complaints, and resort to court action to encourage greater compliance with the law. In addition to investigating thousands of complaints received by individuals, the Commissioner has initiated herself 38 complaint investigations and conducted three audits of PIPEDA-regulated organizations since 2001. Also since 2001, the Commissioner has named companies in the public interest 32 times, and initiated 17 court actions.

Canada's economy depends on trade and the flow of information. PIPEDA may apply to over a million businesses across Canada[13]. However, as globalization creates a more open economy, the Office is no longer dealing solely with Canadian companies. Many are headquartered in other countries, with or without their own regulatory privacy requirements. It is legitimate to question how a small entity with limited resources, such as the OPC, can attract the attention of these companies and proactively encourage them to comply with PIPEDA when the reality is that there are very limited consequences for contravening Canadian privacy law. As the ETHI Committee report pointed out, "it is important that Canadians who use these services (social media) be protected by their own laws and values[14]."

We have made use of the existing tools under the Act, and in some cases, we have been successful in prompting change – but often after we have invested significant resources and almost always after the fact. We have seen some organizations ignore our recommendations until the matter goes to Court; others, in the name of consultation with the Office, pay lip service

to our concerns but ultimately ignore our advice. There is nothing in the law that provides enough incentive for organizations to invest in privacy in significant ways given that they can always renege on their agreement to change their practices and decide not to follow through with the Commissioner's recommendations after the investigation or audit.

The days of soft recommendations with few consequences for non-compliance[15] are no longer effective in a rapidly changing environment where privacy risks are on the rise. It is time to put in place financial incentives to ensure that organizations accept greater responsibility for putting appropriate protections in place from the start, and sanctions in the event that they do not. Without such measures, the Privacy Commissioner will have limited ability to ensure that organizations are appropriately protecting personal information in the age of Big Data.

The national and international context

Several provincial commissioners have order-making powers, in addition to other functions prescribed in their legislation that are similar to those of the OPC, such as carrying out investigations, conducting research or educating business or the public about privacy issues. Order-making powers do not inhibit the ability of those commissioners to perform a range of functions. In fact, this multiplicity of roles is commonplace for many administrative agencies.

In other jurisdictions, there has been a trend towards more robust enforcement powers, and more substantial penalties and fines.

The U.S. Federal Trade Commissioner (FTC) has negotiated a number of high-profile financial settlements over privacy infractions[16]. The United Kingdom, Ireland, New Zealand, and Spain data protection authorities (DPAs) also have order-making power[17], with the United Kingdom and Spain also having the ability to fine organizations. In the United Kingdom, these stronger enforcement powers have not precluded an ombudsman-like approach, where appropriate, and fines have been issued only where a softer touch has failed.

Recent amendments to Australia's *Privacy Act* give the Commissioner the ability to accept enforceable undertakings and apply to the Federal Court for penalties of over a million Australian dollars for a company.

On January 25, 2012, the European Commission released its "Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)." At present, enforcement powers vary widely in the European Union. To bring some uniformity to the powers across the continent, one proposed aspect of the regulation calls for all DPAs to have the power to issue orders to cease specific activities, correct, erase or destroy data and provide individuals with access to their data. In addition to making breach reporting mandatory, the proposed Regulation would empower each DPA to impose administrative sanctions, ranging from warnings to fines[18].

One of the reasons PIPEDA was enacted was to create a vehicle for Canada to provide a level of protection for personal information that would facilitate the flow of personal information from EU member states to Canada. The current EU Data Protection Directive, adopted in 1995, (which the proposed Regulation would replace) introduced a requirement that member states allow transfers of personal information to a third country such as Canada only if the third country ensures an adequate level of protection for that information. The adequacy concept is retained under the Regulation. It is an open question as to what effect the proposed Regulation, if passed

in its present form, might have on Canada's adequacy status, given the current state of PIPEDA[19].

At risk of falling behind

Against the backdrop of these changes, the enforcement model provided for under PIPEDA appears increasingly out of date. When it was introduced in 2000, it was considered a leader among data protection legislation because of its technology-neutral, principled-based approach. We continue to believe that this approach of PIPEDA is its strength. However, the past decade has witnessed the rise of new laws elsewhere that are providing data protection authorities with stronger powers commensurate with the increasing risks to personal information. While at the moment, the Commissioner has the power to name a company in the public interest, which may encourage some companies to adopt her recommendations to avoid negative publicity of offside privacy practices, naming is ultimately only one means of encouraging compliance. Given the reach of, and/or the wealth of personal information held by, organizations (particularly those that operate online), it is challenging for people to "vote with their feet" when increasing amounts of their personal information are being held by fewer and fewer organizations.

With other jurisdictions continuing to move towards granting their data protection authorities the power to award damages, administer fines, make orders, and/or require organizations to report serious breaches, Canada needs powers comparable to those in other jurisdictions in order to have meaningful impact on privacy protection. This is especially necessary given the global nature of today's business environment and the reality that the most powerful players in the digital economy operate internationally.

Canada cannot afford to be left behind, with little in the way of consequences for those that do not respect this country's federal privacy law.

Recommendation 1: Strengthen enforcement and encourage greater compliance

Reform PIPEDA to provide for stronger enforcement powers. These could include statutory damages (administered by the Federal Court); or giving the Commissioner the power to make orders; or affording the Commissioner with the power to impose administrative monetary penalties; or a combination of the above.

There are a number of options that, alone or in combination, could strengthen the current enforcement model and encourage greater compliance with the Act. These include a regime of statutory damages attached to reviewable[20] provisions of the Act listed in section 14 of PIPEDA, administered by the Federal Court. Another option would be to give the Commissioner power to order organizations to do or cease doing something in order to bring themselves into compliance with PIPEDA. A third option would be to afford the Commissioner the power to impose administrative monetary penalties in cases that warrant it. Each of these enforcement options is explored further below.

A. Statutory damages

PIPEDA could be amended to empower a Court to order statutory damages for certain contraventions. Pursuant to this model, damages would be awarded for contraventions of certain PIPEDA provisions, without the requirement for a claimant to prove an actual loss stemming from the contravention. A range of damage awards could be prescribed, setting out minimum and maximum amounts for contraventions of specific provisions. Within that range, courts may assess damages based on a number of explicit factors to be taken into consideration.

From a policy perspective, statutory damages are appropriate in situations in which it is difficult or impossible for a plaintiff to prove a quantifiable loss as a result of a contravention of the law. By setting established ranges or amounts, statutory damages facilitate the Court's deliberations about appropriate amounts, particularly for non-economic loss such as humiliation resulting from a privacy violation. Increased certainty with respect to damage awards that may be available can encourage plaintiffs to enforce their rights before the Courts in appropriate circumstances (and discourage plaintiffs with unrealistic expectations from pursuing court action). Greater certainty in law is also beneficial for organizations in that they will know what they may face and be better able to evaluate risks and predict outcomes.

Statutory damages may be able to accomplish similar policy goals as administrative monetary penalty (AMP) regimes in terms of encouraging organizations, by means of financial incentives, to comply with PIPEDA. However, there are some significant differences. First, statutory damages could be awarded to aggrieved individuals, whereas AMPs are normally payable to the Consolidated Revenue Fund. Second, under a regime of statutory damages, the Federal Court would continue to be the arbiter of damage awards within the parameters set out in statute according to well-established experience and litigation procedures.

Examples of Regimes Involving Statutory Damages

The *Copyright Act* contains a statutory damages regime for infringement of copyright. This regime was amended in 2012, establishing minimum and maximum awards for non-commercial and commercial infringements. For **each** work where the infringement is for commercial purposes, the minimum award is $500 to a maximum of $20,000. In contrast, for non-commercial infringements, the minimum is $100 and the maximum is $5,000 with respect to <u>all</u> works involved in the proceeding.

As another example, Canada's anti-spam legislation, CASL, has established statutory damages in connection with a newly-created private right of action for any breach of CASL or related amendments to the *Competition Act* or PIPEDA. Maximum damage awards range from $200 for each contravention to a maximum of $1 million each day the contravention occurred, depending on the provision in question. This is a noteworthy development in that Parliament has already considered it appropriate to create a statutory damages regime applicable to PIPEDA for specific contraventions.

B. Order-making powers

Order-making powers would allow the Commissioner to issue a binding order to an organization to either do, or cease to do, certain things, in order to redress consequences of a contravention, or to prevent one. In other words, the Commissioner would be able to order what she can now only recommend.

Under the model contemplated here (and as is normally the case for other federal administrative tribunals with order-making powers), if an order is not obeyed the complainant or the Commissioner could register the order with the Federal Court and have it enforced as an order of the Court in accordance with the Court's contempt powers. For its part, the organization could avail itself of judicial review. The scope of provisions over which the Commissioner would be afforded order-making powers would be a question of legislative policy.

Examples of order-making powers in provincial data protection statutes

Alberta, British Columbia and Quebec have legislation that covers the activities of the private sector and is considered substantially similar to PIPEDA. Under those laws, orders can be issued to the private sector with respect to certain actions. The Commissioners in those provinces also have other functions that enable them to perform multiple roles, such as educator; adjudicator; enforcer; advocate and so on.

C. Administrative Monetary Penalties (AMPs)

Administrative monetary penalties (AMPs) are civil penalties or fines that may be issued in response to non-compliance with the law. An AMP is not intended to be punitive. Its intent is largely to encourage compliance, or conversely deter non-compliance, through financial incentives. More than merely a "cost of doing business", AMPs are a timely and effective means of bringing organizations into compliance with the law.

AMPs are imposed by the agency administering the statute, not the courts. If not paid, they become debts to the Crown that may be collected by means of civil action in the courts. The decision to impose an AMP, like any other administrative agency decision, would be subject to judicial review.

AMPs may be considered a distinct instance of an order-making power, but differ from other binding orders in that they oblige the organization to pay a defined sum of money. Statutory AMP schemes typically specify the standard of proof to be on a balance of probabilities and set out maximum and minimum amounts; they may also include a list of criteria to be used in determining the size of the AMP, or grounds which may or may not be invoked as defenses in AMP proceedings. Statutory AMP schemes are sometimes also characterized by specific procedural requirements, timeframes and review or appeal mechanisms.

Examples of Regimes Involving Administrative Monetary Penalties (AMPs)

Since PIPEDA was passed, several AMP regimes have been introduced in Canada. FINTRAC, for example, was created in 2000 to detect, prevent and deter money laundering and terrorist activity financing. In 2008, it was given the authority to issue an AMP to reporting entities that are not in compliance with the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*.

Canada's anti-spam legislation, CASL, also contains an AMP regime. Under CASL, the Canadian Radio-television Telecommunications Commission (CRTC) will be able to impose administrative monetary penalties for violations of up to $1 million per violation for individuals, and $10 million per violation for other persons (e.g., corporations). Businesses that violate related provisions of the *Competition Act* when sending electronic messages can be penalized up to $10 million for a first contravention and up to $15 million for subsequent contraventions. Unlike its partners in the enforcement of CASL, the OPC does not have the ability to seek or impose administrative monetary penalties as an enforcement tool.

Of the other Agents of Parliament, the Conflict of Interest and Ethics Commissioner has the power to levy an AMP on reporting public office holders who do not meet certain reporting requirements under the *Conflict of Interest Act*. The maximum penalty under that Act is $500, with the penalties issued so far ranging from $100 to $300. The *Conflict of Interest Act* is currently under review and our understanding is that the Conflict of Interest and Ethics Commissioner has asked that the AMP scheme be expanded to breaches of the legislation's substantive provisions, and that a higher maximum penalty than $500 be attached to certain contraventions[21].

Pressure Point 2: Breaches and lack of mandatory reporting

The vast quantities of personal information in the hands of organizations can create serious risks to the privacy of the individual. The unanticipated, unwelcome or intrusive uses of personal information as a result of security or privacy lapses in organizations' practices[22] have grown dramatically. To be sure, such breaches are not new. What has changed, however, even since the first review of PIPEDA began in 2006, is the nature, scope and scale of the information at risk[23]. Breaches are a serious threat to Canadians' personal information and to organizations. They risk undermining identity protections and reputation, and they can be expensive for all parties to clean up.

Over the past few years, there have been a number of high-profile data breaches both in Canada and abroad that compromised the personal information of Canadians. There can be many harms stemming from such breaches, including identity theft, financial loss, negative credit ratings, and even physical harm.

While there is some research that suggests that, overall, organizations are expected to increase IT security spending to protect their data assets from theft and attack[24], other research suggests that organizations, particularly those in Canada, are not focusing enough resources in this area[25]. We think more attention needs to be paid to these issues.

Recommendation 2: Shine a light on privacy breaches

Require organizations to report breaches of personal information to the Commissioner and to notify affected individuals, where warranted, so that appropriate mitigating measures can be taken in a timely manner.

Within Canada, Alberta's private-sector privacy legislation, the *Personal Information Protection Act*, and certain provincial health privacy laws, have mandatory breach notification requirements. Organizations subject to PIPEDA, however, are not obliged to report to the federal Privacy Commissioner. While some choose to voluntarily report, as well as inform individuals of the breach (in appropriate cases), many do not, leaving affected individuals at risk. Until there is a mandatory notification requirement, which can bring the number, nature and size of privacy breaches out in the open, the full picture remains opaque.

What is clear, however, is that the current situation creates an uneven playing field for organizations. Those that report may face reputational damage and the expense of cleaning up, while those that do not report may potentially escape with no negative effects on their reputation or bottom line.

Canadians' expectations are also noteworthy. In the 2012 survey conducted by the OPC, 59% of respondents think it unlikely that an organization would notify them in the event of a breach. However, nearly all surveyed, 97%, stated that they would want to be notified in such circumstances[26].

In recent years, other international jurisdictions have developed new approaches to dealing with serious privacy breaches and have taken measures to shore up their privacy frameworks. For example, the United States has been a leader in developing mandatory breach notification legislation, with most states having passed mandatory notification legislation. As noted earlier, the United Kingdom also has the ability to fine organizations in relation to serious breaches. Early in 2013, the UK Information Commissioner's Office issued a £250,000 fine against Sony for a breach that affected the personal information of millions of Playstation users.

All member states in the European Union are required to implement breach notification laws with respect to telecommunications companies and other providers of electronic communications services. The proposed European Union Regulation would expand this to cover other organizations.

Mandatory breach provisions[27] would therefore bring PIPEDA in line with many other jurisdictions.

In addition to making it mandatory for organizations to report breaches to the OPC and to inform individuals in accordance with applicable thresholds, the failure to notify should be made a reviewable provision, along with the failure to establish security safeguards, and subject to stronger enforcement, as described Section 1, above.

Pressure point 3: "Lawful authority" disclosures and lack of transparency

Paragraph 7(3)c.1 of PIPEDA states that an organization may disclose personal information to a government institution or part of a government institution without the knowledge or consent of the individual if the government institution has requested it; has identified its "lawful authority"; and has indicated one of the following:

(i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs;
(ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law; or
(iii) the disclosure is requested for the purpose of administering any law of Canada or a province.

This clause was inserted in the final phases of Parliament's consideration of PIPEDA, in 1999, specifically at the request of police and governmental authorities to ensure that long-standing relationships with companies could be maintained.

At present, under this provision, companies have the discretion to challenge or refuse such requests under PIPEDA; many have done so where they believe the requesting authority ought to first obtain a court authorized order. However, others may be less resistant given the broad language of paragraph 7(3)c.1 as currently worded. Specifically:

- The term "government institution" is not defined and could apply to any number of provincial or federal organizations; likewise, the term "lawful authority" is undefined;
- The threshold for the "purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying our an investigation relating to the enforcement of any law, or, gathering intelligence for the purpose of enforcing any such law" outlines broad parameters for potential requests; and
- The act of "administering any law of Canada or a province" is also broad.

We have no way of knowing for certain the number, scale, frequency of, or reasons for, such disclosures although we understand that they are substantial. There are no provisions requiring organizations to report on these disclosures, and Canadians seeking access to their personal information would likely be unable to find out if their personal information had been disclosed under paragraph 7(3)c.1 given access prohibitions outlined in subsection 9(2) of PIPEDA.

This regime is troubling from a privacy standpoint given that there is no transparency or any established rules about what personal information can or should be provided to government institutions without authorized court order or judicial warrant. Given the sheer volume of personal information held by organizations, the risk to privacy from such warrantless disclosures is substantial and merits reconsideration.

Recommendation 3: Lift the veil on authorized disclosures

Require organizations to publicly report on the number of disclosures they make to law enforcement under paragraph 7(3)(c.1), without knowledge or consent, and without judicial warrant, in order to shed light on the frequency and use of this extraordinary exception.

Canadians have expressed significant concerns about warrantless access by law enforcement to personal information. It is increasingly apparent that greater transparency is needed with respect to this provision. Organizations should at a minimum be required to keep a record of tombstone data related to such disclosures, and they should be required to post in a publically available fashion, the number of such disclosures that they make on a quarterly basis. Such public accounting could take the form of postings on the organization's website. Some organizations have already started taking the lead on transparency in this regard[28].

Pressure Point 4: Demonstrating accountability

PIPEDA was one of the first data protection law to explicitly reference and elaborate on the accountability principle. PIPEDA was largely influenced by the Organisation for Economic Co-operation and Development's (OECD) 1980 *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, which included the first expression of the accountability principle[29].

The accountability principle has been included in the Asia-Pacific Economic Cooperation's (APEC) Privacy Framework and the concept of accountability has also attracted interest in Europe. The new proposed European Union legal framework contains a provision that concerns accountability, including a requirement to be able to *demonstrate* accountability.

US business interests have also driven the debate about accountability in recent years, hoping to make international transfers of personal information to and from Europe easier. Many of the same parties have taken an interest in the Canadian model and approach.

The OPC, along with our counterparts in Alberta and British Columbia, issued guidance[30] on what we think an accountable organization's privacy management program should contain.

Proactive compliance

While PIPEDA requires organizations to be accountable for their privacy practices and procedures, and specifies how to do so, there is very little within the legislation to encourage and reinforce proactive compliance. Too often, our investigations have revealed organizations that have repeatedly failed to adapt their privacy governance processes to address certain problems, in some cases even after we had investigated them. Some of these problems would have been obvious if the product or service had been examined more carefully from the start.

For example:

- A first complaint against a major retail company was filed in October 2004; another complaint by a different individual was filed against the same company in February 2006. Both complaints concerned the inadequacy of the company's measures to remove personal information from devices that had been returned to the organization and then resold. Both times, the Commissioner made recommendations that the company agreed to implement. After media reports surfaced in 2009 involving yet again the same organization and the same issue, the OPC conducted an audit. It was only at the conclusion of that audit in 2011 – nearly seven years after the first complaint was filed – that the company effectively addressed the issue.

- We have seen a number of complaints of inappropriate activities on the part of some employees in the financial sector. The employees appear to be ignoring the companies'

procedures for protecting customer personal information in spite of their organizations' privacy management regime. Although each case in isolation appears to be a one-off employee error, when taken together, there appears to be systemic re-occurrences that must be more effectively addressed through reinforced governance structures and processes.

- On more than one occasion, some organizations have shown that, in their rush to put services and products on the market, they have not fully anticipated the many privacy challenges these services and products would have and failed to take the necessary steps to address these challenges at the outset of product development.

- In a study undertaken by the OPC on "web leakage", one in four websites that we tested were either unaware that they were disclosing information to third parties or were not clearly informing Canadians that they were transferring personal information to service providers[31].

The above examples are not unique. We believe that privacy is not given as prominent a place in business practices as it should, given the importance of confidence and trust in the digital economy and the pivotal role that personal information plays.

Given the complexity of personal information handling, the sheer volume of personal information involved, and the need on the part of organizations to have the flexibility to implement the privacy principles outlined in the Act, organizations must create better privacy management programs that are diligently and consistently followed. Privacy issues require more attention within organizations so that the personal information of Canadians will be better protected, and the embarrassments and expenses, after the fact, are avoided. More prominence for privacy is needed to support the work of privacy professionals within organizations.

Accountability for implementing recommendations

The Commissioner's ability to follow up with organizations that have agreed to implement her recommendations following an investigation can lead to some uncertainty and administrative challenges for the Office.

Ensuring that organizations honour their commitments with respect to recommendations has become an increasing burden on our Office, taking a great deal of time and resources. While technically our investigations are over when the Commissioner issues her findings, Canadians need to know that organizations are taking their responsibilities seriously after the investigation is over. Monitoring and analyzing a company's actions, however, can be almost as time-consuming as an investigation.

For example, our follow up with Facebook, after the release of our 2009 investigation findings, required significant resources and took an additional full year. Another notable follow-up has involved Nexopia. More than a year after releasing the findings, we were monitoring the company's commitment to implement the 24 recommendations we made.

Under PIPEDA, the Commissioner or the complainant has 45 days in which to apply to Federal Court to have the Commissioner's recommendations enforced. Often, complex recommendations cannot be implemented within the 45 day timeframe, particularly in those cases requiring technological solutions. While such court applications may be filed beyond the 45 day time limit, this can only be done with leave of the Court.

Recommendation 4*: *Walk the talk

Modify the accountability principle in Schedule 1 to include a requirement for organizations to demonstrate accountability upon request; to incorporate the concept of "enforceable agreements"; and to make certain accountability provisions subject to review by the Federal Court.

The existing Accountability Principle under PIPEDA could be strengthened to improve personal information protection for Canadians.

Demonstrating compliance

A fundamental tenet of accountability is that organizations must be able to demonstrate to oversight bodies, upon request, that they have a program in place to ensure that their practices are compliant with privacy law. PIPEDA does not currently have such a requirement. We are of the view that the law should be amended to require organizations to demonstrate, at the Commissioner's request, that they have a privacy program in place. Such a change would bring the legislation in line with the direction that the European Union is taking in this regard.

It may be time to consider how the concept of accountability could be used as an incentive for compliance with PIPEDA. An organization will be more inclined to take its accountability, and therefore its privacy obligations more seriously when the consequences for not doing so hit its bottom line.

Requiring organizations to demonstrate that they are accountable may create incentives for them to truly "walk the talk". For example, should there be an investigation or a breach, a demonstrably functioning, up-to-date privacy management program[32] (which should include privacy impact assessments) may constitute a mitigating factor when assessing damages.

Trustmarks and third-party certifications could also be explored. Under such schemes, an organization shows that it adheres to certain practices in order to earn the certification or mark. These schemes have, however, been subject to criticism for a lack of enforcement.

Enforceable agreements

PIPEDA should be amended to explicitly introduce the concept of "enforceable agreements," in which an organization, at the end of an investigation, would agree to comply with the Commissioner's recommendations and to demonstrate such compliance within a set time period. The Act could also be amended to address what recourse the OPC would have should the organization not honour its commitments. In this way, there could be improved personal information protection for individuals that also allows for a more effective and efficient use of public resources by the Office.

It would bring greater certainty and may ease the burden on the Office with respect to follow up to have clear obligations on the part of the organization to demonstrate its implementation of the recommendations to the OPC and to have clear options for recourse should that not occur.

Other possible changes

Another possible modification to PIPEDA to strengthen organizational accountability and give it meaningful effect could involve bringing more of the accountability-related principles from Schedule 1 into the scope of reviewable provisions under section 14 that may be subject of review before the Federal Court. Currently only Principle 4.1.3 is reviewable[33].

CONCLUSION

Parliament enacted PIPEDA to allow the digital economy to flourish by helping Canadians feel secure in using the Internet as a means to conduct business and obtain information. It is a technology-neutral and principles-based law – characteristics that must remain as we move further into the 21st century.

However, in our view, it is becoming increasingly clear that the balance intended by PIPEDA is no longer there. Too often, the privacy rights of individuals are displaced by organizations' business needs. At this stage in PIPEDA's evolution, incentives are needed to encourage organizations to build robust privacy compliance in the early stages of product or service development and sanctions should be levied in the event something goes wrong.

Given the remarkable changes in how personal information is collected, used and disclosed by organizations as well as the global nature of today's digital economy, Canada's federal private-sector privacy law needs strengthening in ways that will make it comparable to privacy protection laws elsewhere in Canada and the world.

It is in the interest of both consumers and businesses to support a thriving digital economy in which people can actively participate, knowing and trusting that their personal information will be respected.

ENDNOTES

[1] From Industry Canada's website: Privacy for Business, Electronic Commerce in Canada.

[2] From the Honourable John Manley's speaking notes, presentation to the Senate Committee Studying Bill C-6, December 2, 1999.

[3] PIPEDA does not apply to organizations that collect, use or disclose personal information entirely within provinces that have substantially similar legislation – Alberta, British Columbia and Quebec (and Ontario, New Brunswick and Newfoundland and Labrador, in respect of personal health information collected, used or disclosed by health information custodians.) PIPEDA covers other commercial activities in the latter three provinces. Where it exists, the substantially similar provincial law will apply instead of PIPEDA, although PIPEDA continues to apply to interprovincial or international transfers of personal information and to personal information held by FWUBs.

[4] Privacy and Social Media in the Age of Big Data

[5] Canadians' Internet usage nearly double the worldwide average

[6] 2.5 Quintillion Bytes Created Each Day, Calculated ViaWest

[7] Bringing smarter computing to big data

[8] For example, prior to being purchased in 2012 by Facebook, Instagram, a photo hosting site, boasted around 13 employees. In 2011, Instagram had 5 million users.

[9] "How companies learn your secrets," Charles Duhigg, *New York Times*, February 16, 2012

[10] See, Survey of Canadians on Privacy-Related Issues

[11] Page 6 of the *ETHI Committee Report on Privacy and Social Media in the Age of Big Data*.

[12] Canada (Privacy Commissioner) v. Blood Tribe Department of Health, [2008] 2 S.C.R. 574, 2008 SCC 44

[13] The Business Register only includes companies that meet at least one of the following conditions: "it must have at least one paid employee (with payroll deductions remitted to the Canada Revenue Agency (CRA)), it must have annual sales revenues of $30 000, or it must be incorporated and have filed a federal corporate income tax return at least once in the previous three years."

There were approximately 2,428,270 businesses in Canada – if you remove the businesses in Quebec, Alberta, and BC, there are 1,217,410 that are under PIPEDA's jurisdiction.

[14] Page 7 of the *ETHI Committee Report on Privacy and Social Media in the Age of Big Data*.

[15] While an individual may now take a company to court, damage awards under PIPEDA to date have been low.

[16] Google agreed to pay a $22.5 million penalty to settle FTC charges over misrepresentation to Apple's Safari browser users regarding the placement of cookies, which was a violation of a previous settlement with the FTC over Google's privacy practices.

[17] This is not an exhaustive list.

[18] This information is accurate as of May 8, 2013.

[19] A draft report from the EU Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), proposed amendments to the Regulation that would require that "sufficient sanctioning powers" on the part of the supervisory authorities in the other jurisdiction be in place in order for an adequacy finding to be made. The LIBE Committee and four other committees comment on the Regulation. The review of the Regulation continues.

[20] Under section 14 of PIPEDA, a complainant may apply to the Federal Court for a hearing regarding a matter complained about or referred to in the report the Commissioner issues after her investigation. Such an application must relate to specific sections of PIPEDA or principles under Schedule 1, which are listed in section 14. These are referred to as "reviewable" provisions.

[21] See page 70 of the Commissioner's submission to the ETHI Committee, where it is suggested that the maximum penalties in certain cases (namely "substantive contraventions" where it is clear that the contravention occurred and no full examination is warranted) "could be higher than the existing $500 limit."

[22] OECD (2011), "The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines", OECD Digital
Economy Papers, No. 176, OECD Publishing.

[23] In one data breach suffered by Sony, 77 million user accounts containing names, addresses and possibly credit card data, were stolen.

[24] Global security spending to hit $86B in 2016

[25] "Canada is lagging behind most countries in security innovation, with little more than 5% of spending invested in new technologies and management processes targeting information security over the last 12 months."

[26] See, Survey of Canadians on Privacy-Related Issues.

[27] Bill C-12 contains mandatory breach notification provisions. As of the date of this document, it is in Second Reading.

[28] See, Google's Transparency Report; Microsoft's 2012 Law Enforcement Requests Report; and Twitter's Transparency Report.

[29] It appears that some further consideration of accountability may form part of the review of those Guidelines, which is currently under way. See the Terms of Reference for the Review of the OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data, October 31, 2011.

[30] See, Getting Accountability Right with a Privacy Management Program

[31] See, OPC "web leakage" research project

[32] For more information on what the OPC considers to be the elements of a strong privacy management program, please see, *Getting Accountability Right with a Privacy Management Program*, issued by the OPC and the Alberta and British Columbia Information and Privacy Commissioners Offices in April 2012.

[33] Under 4.1.3, an organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.