

PRIVACY PRIORITIES

Reflections on the Office of the Privacy Commissioner
of Canada's Strategic Priority Issues



Office of the
Privacy Commissioner
of Canada









Office of the
Privacy Commissioner
of Canada

This document highlights only a small selection of work we did within the scope of our strategic priorities. A longer version of the report, which includes a comprehensive inventory of all our activities, is available on our website.



Contents

2		Commissioner's Message
7		PRIORITY Public Safety and Privacy
17		PRIORITY Information Technology and Privacy
25		PRIORITY Identity Integrity and Protection
35		PRIORITY Genetic Information and Privacy
43		The Road Ahead

COMMISSIONER'S MESSAGE

One of the most significant challenges faced by a privacy regulator in the 21st century is the fact that there are so many new risks to privacy – most of them unfolding at breakneck speed in ways we could not have imagined just a few years ago.

Indeed, the privacy landscape is in constant and dramatic evolution.

In order to meet this challenge as effectively as possible, my Office decided in 2007 to identify key strategic priorities that would serve as focal points for our work.

After a careful, deliberative process, we identified: 1) information technology; 2) public safety; 3) identity integrity; and 4) genetic information as our key areas of focus in this era of rapid change.

These priorities have helped us prioritize incoming requests and demands on our Office, develop our work plans, and leverage our resources where we could have the greatest impact for Canadians.

SELECTING OUR FOUR PRIORITIES

As we set out to identify our strategic priorities, we considered several criteria.

We assessed several potential priority issues in terms of their intrinsic importance: whether they were national or international

in scope; their relative urgency; and relevance to Canadians.

We considered our potential role in advancing the issue: whether the matter was appropriately within federal jurisdiction; whether it was well-aligned with our mandate and relevant to both public and private sectors; what type of leadership was needed; and what our Office's value-added contribution might be.

Finally, we considered matters of practicality, such as: the opportunity for us to have meaningful impact; the feasibility of achieving results within three to five years; what past investments we could leverage going forward; and who potential partners might be.

As a result of that process, a consensus developed around the following four strategic priorities with very significant implications for privacy:

- > Public safety and privacy
- > Information technology and privacy
- > Identity integrity and protection
- > Genetic information and privacy

At the time, we saw in each of these areas the potential for evolving social norms and business models to have significant impacts on privacy rights.

We anticipated the appetite for personal information to grow exponentially and the drive for innovation to forge ahead globally at lightning speed.

We saw the opportunity for our Office to participate actively in the public debates needed to raise privacy concerns in a timely way. We set out to encourage government institutions and private sector organizations to build in necessary protections to minimize privacy risks in these areas. We saw our role as enabling responsible progress and innovation in a manner that respects privacy rights, and ultimately earns and maintains the trust of Canadians.

ALLOCATION OF RESOURCES AND PRIORITY FOCUS

For each priority, we created a working group comprised of staff from across the various branches of the Office. The four working groups met regularly to discuss relevant issues, share information, and learn from outside experts.

Organizing our work according to these four priorities allowed us to allocate our resources in a way that would maximize beneficial impact for Canadians.

For example, it guided our decisions in terms of which investigations to initiate; privacy compliance audits or privacy impact assessment reviews to prioritize; research projects to undertake and/or fund through our Contribution Program; guidance materials to issue; and public and stakeholder outreach activities to focus on.

It also bolstered our capacity in these areas, which put us ahead of the curve in terms of our policy work, our advice to Parliament,

our guidance for businesses and individuals, and our readiness to foresee and respond to emerging issues.

VITAL IMPACT

Canadians today face threats to their privacy that are varied and vast.

With respect to our four strategic priorities, I am pleased to say that we have made significant strides in raising public awareness of these novel issues in both the public and private sectors.

We have used the compliance and education tools at our disposal to encourage government institutions and private sector organizations to develop policies and adopt practices that are more respectful of privacy than they would otherwise have been.

We have also expanded our own knowledge and built internal capacity around these key privacy issues through proactive research efforts – believing that it is essential to take time to fully understand changes that impact on privacy and stay ahead of the curve, rather than fall behind.

MAKING CONNECTIONS

When we started this exercise, many of us saw these four priority areas as quite distinct. However, we now recognize many connections that have revealed themselves in recent years.

All four of these priority areas have been swept up in the groundswell of Big Data. Whether

it be massive collection and aggregation of travel and security-related information; choice of friends, links, tweets, likes and dislikes garnered through social media; consumer online purchasing patterns and web-searching behaviours; whole genome-sequence analyses of entire populations – we are seeing a significant paradigm shift in how personal information is collected, used and fundamentally understood.

Personal information has become the common currency that drives this new phenomenon.

In an article in *Foreign Affairs*, Kenneth Cukier and Viktor Mayer-Schoenberger summed up this new phenomenon as follows:

Big data is posed to reshape the way we live, work and think. A worldview built on the importance of causation is being challenged by a preponderance of correlations. The possession of knowledge, which once meant an understanding of the past, is coming to mean an ability to predict the future. The challenges posed by big data will not be easy to resolve. Rather, they are simply the next step in the timeless debate over how to best understand the world.¹

While I recognize the tremendous societal benefits that could come from this quest for new forms of knowledge, as Privacy

¹ Kenneth Cukier and Viktor Mayer-Schoenberger, "The Rise of Big Data : How It's Changing the Way We Think About the World," *Foreign Affairs*, 92 (2013): 28-40.

Commissioner of Canada, my job is to identify the privacy risks involved, and work to mitigate them on behalf of Canadians.

My Office strives to help enable responsible progress while protecting Canadians' personal information from potential misuse in the hasty push towards profit or expedience.

Over time, I have come to see these issues at their core as ethical issues about the way we understand the world around us, the respect we hold out for individuals' right to autonomy and dignity, and the kind of society we want to live in.

CONCLUSION

Several years after identifying the strategic priorities, and as my mandate comes to a close, it is time to take stock.

In hindsight, were these four issues the right ones to focus on? What have we learned about them? Has our Office made a difference in these areas? If we were to re-do this same priority-setting exercise today, would we come up with the same or different priorities?

By any measure, we believe the strategic priorities initiative has been a success.

The pages that follow highlight a few of our achievements that have had a real impact in protecting the privacy rights of Canadians.

I will be leaving the Office of the Privacy Commissioner of Canada at the end of 2013 after a decade at the helm. I offer these

observations in the hope that they may offer some helpful insights for protecting privacy in the years to come.

The new Commissioner will begin with a clean slate and will determine the priorities of the next mandate. I am confident that the Office and its remarkably talented in-house experts will continue to build on the solid foundation we have already put in place – no matter what new challenges the future brings.

Finally, I would like to take this opportunity to thank my hard-working staff for their passion for privacy, their dedication to the standards of excellence and the ethical behaviour Canada expect in its civil service, and also for their exceptional work on our four strategic priorities over the years.

We have come a long way.



JENNIFER STODDART

Privacy Commissioner of Canada



D
Gates/Portes



i Information



Ground Level Rezervasi

PRIORITY CHECK-IN
Enregistrement prioritaire
Canada / 1-800-387-8324





PRIORITY

PUBLIC SAFETY AND PRIVACY

HOW IT BEGAN

The September 2001 terrorist attacks on the United States spurred a dramatic increase in national security measures across North America, including at the Canada-U.S. border.

With a stunning escalation in technological capabilities, authorities seek to hold terrorism and crime at bay by monitoring what people say and do, detecting suspicious behaviour and even predicting their intentions.

From the start, our Office realizes that the right to privacy, though fundamental, is not absolute. It must be exercised in relation to other fundamental rights – in this case, the right to live one's life secure from threats of harm.

Public safety and privacy are not at odds. Rather, they must both be integrated and accommodated so that they may continue to coexist in a free and democratic society.

WHAT WE OBSERVED

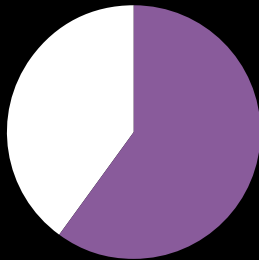
Our work in this area revealed how the capacity of public safety agencies to collect and store vast amounts of personal data has increased substantially.

Technological developments have resulted in a new generation of mobile devices, remote sensors, high-resolution cameras and analytic software – all of which have revolutionized surveillance techniques.

BY THE NUMBERS

A poll conducted for the Association of Canadian Studies in late 2012 found that 60 percent of respondents disagreed with the statement:

“in order to curb terrorism in this country, I am ready to give up some civil liberties.”



60%
disagreed

Terrorism and counter terrorism: Knowledge, Fears and Perceived Causes. Association for Canadian Studies. December 2012 <http://www.acs-aec.ca/en/>

Technology has also enabled the development of a vast range of ever-bigger and increasingly sophisticated personal information databases.

Huge amounts of personal information – for example, communications traffic, financial transactions and air travel itineraries – are collected, shared, matched and analyzed for public safety purposes. And all of this activity unfolds at the speed of light.

Our Office has held that public safety authorities must be accountable to a degree appropriate to the significant powers entrusted to them.

As well, the exercise of such powers must be in line with fundamental rights and Canadian values. Without such limits, the very basis of our free and democratic society – trust between the state and its citizens – would be threatened.

WHAT WE ACHIEVED

Rather than examining each new public safety measure as it arose, designating Public Safety and Privacy as a priority issue allowed us to take a more comprehensive, well-balanced, integrated and ultimately effective approach.

We saw our role as working to ensure that new public safety measures, though important in this modern context, do not unduly erode privacy rights.

We did not set out to stop initiatives, but rather, worked to mitigate their potential negative impacts on privacy by asking questions, challenging assumptions and critically examining the issues.

In particular, our work shone a light on public safety initiatives, encouraging greater

transparency and accountability on the part of government departments. We also helped Canadians better understand the implications of security measures on their privacy.

At the same time, we have supported and informed the work of policymakers and Parliamentarians by identifying privacy concerns with respect to proposed public safety legislation. We believe our input was valued and carefully considered, and ultimately led to better informed decision-making.

In most cases, we believe the end result for Canadians has been a more privacy respectful approach to public safety issues.

Here are some examples of our work:

A Matter of Trust

In 2010, we published a reference document entitled *A Matter of Trust: Integrating Privacy and Public Safety in the 21st Century*.

This publication lays out an analytical framework to guide Parliamentarians, policymakers and program designers to be able to incorporate both public safety and privacy.

It begins with the underlying premises and principles, then sets out the checks and balances that ought to inform any new initiative that could infringe on people's privacy.

Before authorities unveil a new measure to boost public safety at the possible expense

of privacy, we encourage them to ask themselves four questions: Is the initiative truly necessary? Would it be effective for the desired purpose? Would any resulting infringement on privacy be proportionate to the expected benefit derived? Are there any other less intrusive alternatives available?

Airport Body Scanners

Most travellers through Canadian airports are familiar with the whole-body imaging scanners that can detect non-metallic weapons, explosives, or other threats to aviation safety.

Their privacy is better protected as a result of the consultations that the Canadian Air Transport Security Authority, or CATSA, had with our Office.

After reviewing CATSA's plans as outlined in a Privacy Impact Assessment, we suggested a variety of privacy enhancements, which CATSA adopted.

For example, passengers have the right to choose a physical pat-down instead of a scan, and scanners are only used as a secondary measure, once a specific threat has been identified. What's more, the images are deleted once an official has confirmed that there is no threat.

In 2011, we conducted an audit and confirmed that the scanned image cannot be reproduced and is permanently deleted after the passenger has left the scanning area: We

also made additional recommendations to further enhance privacy protections.

Our Office recommended the adoption of Automated Target Recognition software, which creates stick figure images of people being scanned.

In 2013, the federal government announced the adoption of that software.

Canada-U.S. Border Initiatives

The governments of Canada and the United States have been developing a perimeter security initiative, the stated goal of which is to increase security and ease trade along our shared border. Prime Minister Stephen Harper and U.S. President Barack Obama signed the Beyond the Border Declaration in 2011.

Our Office has strongly advocated that all initiatives flowing from the agreement must truly and properly integrate and respect the privacy rights expected by Canadians.

We participated in the government's public consultation and submitted a series of recommendations touching on the privacy risks stemming from the various elements of the perimeter security model.

As we stated in our submission, Canadians have high expectations of privacy and a deep commitment where personal information protection is concerned. Given these

sensitivities around private information and sovereignty, we would tend to believe any movement away from these norms would quickly overshadow public debate around plans to follow.

We stressed that any information exchange be: limited to the specific elements of personal information that are truly necessary; constrained in its use and disclosure for very specific purposes; and subject to a robust set of safeguarding measures and oversight.

We also strongly advised that privacy impact assessments should be carried out for individual initiatives flowing from the Beyond the Border Action Plan dealing with personal information.

Following those consultations, the Canada-U.S. Perimeter Security Action Plan was released. We noted that it committed to each country respecting the other's sovereignty, and the right to independent decision-making and risk assessment. The plan also called for each country to maintain its own independent databases.

We are pleased to see Canadian departments and agencies are now regularly consulting our Office and submitting privacy impact assessments for review and recommendations.

We are currently reviewing seven privacy impact assessments related to the action plan and have completed 12 reviews to date.

Have Identification and
Documentation Ready

Ayez vos papiers
d'identité et vos documents
à portée de la main



The Rest of the Iceberg

This section highlights just a few of the activities our Office engaged in under the rubric of the Public Safety and Privacy strategic priority. Please refer to our special web page for a complete inventory of initiatives, including audits of the RCMP exempt databank, RCMP operational databases, government data disposal practices, CATSA, Canadian passport operations, and the Passenger Protect Program (better known as the 'no-fly list'). Other work explored the privacy issues raised by changes in Canada-U.S. border policies; strengthened privacy protections for users of enhanced driver's licences and Indian Status Cards; and examined government efforts to introduce lawful access legislation.

FINTRAC Audit

In order to detect and deter money laundering and terrorist financing, tens of thousands of enterprises operating in Canada are obliged by law to collect personal information of their clients and to report certain financial transactions to the federal Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).

In 2009, we conducted an audit to assess whether FINTRAC has appropriate controls in place to protect personal information, and whether its processes and practices for managing such information comply with the *Privacy Act*. Canadians must be assured that their personal information is being appropriately managed within well-established controls. The requirement

to safeguard personal information, while common to all government departments, is heightened for organizations such as FINTRAC.

We found that, while FINTRAC itself has appropriate systems for collecting and managing personal and financial information, some reporting entities were all too eager to turn over data, sometimes with only the flimsiest justification.

We noted that FINTRAC receives and retains information beyond that which is directly related to its operating programs and activities. Current controls, including front-end screening and ongoing monitoring of reports, need to be enhanced to limit FINTRAC's information holdings.

Lawful Access

Our Office understands the challenges faced by law enforcement authorities in fighting online crime at a time of rapidly changing communications technologies, and the need to modernize their tactics and tools accordingly.

However, we have had significant concerns with respect to the federal government's proposals to address the issue of lawful access.

The government's Bill C-30 would have enabled law enforcement to gain warrantless access to subscriber information, such as an IP address. The Bill's proponents suggested this was akin to information in a phone book.

Our Office's technologists looked at the degree of privacy intrusiveness in relation to the specific information that the Bill had proposed to make readily accessible to police.

In a technical analysis research paper published on our website, we showed how an IP address can, in fact, provide a starting point to compile a picture of an individual's online activities including, for example, online services for which an individual has registered, personal interests based on websites visited, organizational affiliations and even physical location.

Canadians reacted strongly against Bill C-30 and expressed their concerns that it would have a significantly negative impact on their fundamental right to privacy.

We were pleased to see that the government responded to those concerns, announcing in February 2013 that Bill C-30 would not be proceeding in Parliament.

Parliamentary Submissions

Over the years, our Office has appeared before Parliamentary committees to share our views on many proposed pieces of public safety legislation and reviews, such as Canada's Anti-Terrorism legislation. We have also offered our insights in testimony and submissions to federal commissions of inquiry such as the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182.

WHAT IT MEANS FOR YOU

Security and privacy are not mutually exclusive; we can have both. In fact, we argue they must be mutually reinforcing to protect the democratic society in which we live.

Since designating this area as one of our strategic priorities, we have been focusing our efforts to bring legislators and public safety agencies on board with this more balanced approach.

Our work under this strategic priority has strengthened our own insights into the issues.

It has reinforced our credibility among public safety agencies, governments and the public. This has enabled us to open vital channels of communication with these stakeholders, to ensure that privacy concerns remain front and centre.

Our efforts have shown that the relationship between public safety agencies and the people they protect is built on trust. People will generally accept some level of inconvenience, including some sacrifice to their privacy, provided the state is acting with transparency, accountability and integrity.

Essentially, this means treating the personal information of Canadians with the utmost care and respect they deserve.

LOOKING AHEAD

If buttressing privacy rights against the imperatives of public safety is difficult today, it would be illusionary to think things will be simpler tomorrow.

Cybercrime and cyber-espionage are posing challenging new threats to the digital infrastructure that supports our daily lives, including data breaches of staggering proportions.

In countering such dangers, authorities are using ever more surveillance, analytics and other technologies to collect, store, mine and share personal information, often beyond the reach of oversight bodies.

We are hopeful, however, that a principled framework, based on values Canadians cherish in a free and democratic society, can be usefully applied to help integrate privacy protections with public safety and national security objectives.

•REC





INFORMATION TECHNOLOGY AND PRIVACY

HOW IT BEGAN

Information technology was an obvious choice as a strategic priority because so many of the privacy issues that we encounter these days contain a technology component.

In this Digital Age, it is impossible to effectively address privacy issues without understanding the technology behind them.

Technology is evolving at a blinding pace, and the privacy implications of emerging technologies are not always immediately apparent.

Our mission, therefore, was to proactively identify emerging technological developments and get ahead of the curve as

best we could. We needed to build internal capacity required to analyze and understand the market drivers and their privacy implications. Only then could we speak credibly on the related privacy risks and prompt organizations and individuals to take the necessary steps to mitigate them.

WHAT WE OBSERVED

Whether in the fields of education, health, government, commerce, or just around the house, technology is everywhere. Where once we wouldn't leave home without a wallet, it is smart phones and tablets that are becoming indispensable for many Canadians.

As technological devices become more portable, they are also growing more powerful.



BY THE NUMBERS

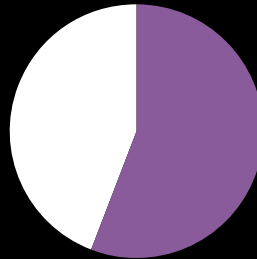
A survey conducted for our Office in 2012 found that three in four Canadians overall—and 92 percent of young people—carry mobile devices such as cell phones, smart phones or tablets.

However, only 56 percent lock it with a password,

and even fewer adjust the settings of the device or its apps to restrict the amount of personal information that gets shared with others.



3 in 4
carry mobile
devices



56%
lock them

Survey of Canadians on Privacy-Related Issues
Final Report, Prepared for the Office of the Privacy
Commissioner of Canada by Phoenix SPI 22013
http://www.priv.gc.ca/information/por-rop/2013/por_2013_01_e.asp

They are able to serve more functions that used to be carried out by several different gadgets. As a result, we're seeing a concentration of personal information in tiny instruments that are easily lost or stolen – a self-evident privacy risk.

Moreover, with many employees carrying around smart phones from work, there is a heightened threat to the security of personal information held in corporate or government records.

Data is also converging in other ways: for example, on a single online platform such as Facebook, or a single service provider, such as Google. In such an environment, the capacity of users to control their personal information is dwindling.

What's more, as technology becomes 'smarter' and more user-friendly, it tends to fade into the background. That's pleasant for users, but it also makes it harder to know that their personal information is being collected and used.

Indeed, between global positioning systems (GPS), radio frequency identification (RFID) technologies, online tracking software that can analyze search histories and equipment that can read biometric indicators, the average person is unwittingly emitting vast amounts of personal information.

WHAT WE ACHIEVED

Given the dazzling scope of technology-related issues, we recognized the importance of building knowledge.

We created a specialized technology lab, held public consultations on specific emerging trends, and conducted international research on new information technologies.

The knowledge we have built has been critical to allowing us to engage with organizations on an equal footing with respect to highly technical issues and put forward credible, well-balanced positions on issues.

Over the years, we have been able to translate our knowledge of technology issues into targeted guidance and public awareness products, and have drawn from that knowledge to inform our investigations and audits, as well as our new responsibilities under Canada's new anti-spam legislation.

Here are some examples of our work:

Technology Analysis Branch

We created a Technology Analysis Branch with specialized staff and a laboratory to carry out the technical analyses needed to support the Office's work.

Thus, for instance, our technologists can assist our investigators in assessing technical elements of a complaint such as privacy options or default settings, certain features of online services, the effectiveness of security safeguards, or claimed data deletion practices.

The Technology Analysis Lab is also an early testing ground for researching new apps and other emerging technologies with potential

implications for privacy, even before they become the object of a privacy complaint.

Our technologists have also provided technical assistance to help our Office prepare for new enforcement responsibilities flowing from *Canada's Anti-Spam Legislation* (CASL). The enforcement of CASL will be shared with the Competition Bureau and the Canadian Radio-television and Telecommunications Commission; our specific role will be to oversee the unauthorized collection of personal information, either through the harvesting of e-mail addresses or the planting of spyware on people's computers.

Social Networking

The exploding popularity of social networking spurred an investigation into the privacy practices of social networking giant Facebook.

As a result of our investigation, Facebook retrofitted its application platform to prevent any app from accessing information without first obtaining express consent from users. In response to another concern about transparency, Facebook agreed to give users more privacy information and improved privacy tools.

That investigation was important for many reasons. We were the first data protection authority in the world to conduct a comprehensive investigation of the privacy policies and practices of Facebook. We established that social networking sites raised

The Rest of the Iceberg

This section highlights only a small selection of work we did within the scope of the Information Technology and Privacy strategic priority. A comprehensive inventory of all our activities is available on our website. For example, you will find there descriptions of our research into web leakage, our deep packet inspection essay project and submission to the Canadian Radio-television and Telecommunication Commission (CRTC) on deep packet inspection. You will also find our guidance on videogames and a wide range of fact sheets on everything from cookies to the hijacking of personal information online. There are also a number of investigations where information technology was a key issue.

fundamental privacy issues and that these sites would be held accountable for meeting their privacy obligations.

Facebook agreed to make changes to its privacy practices that benefitted millions of users around the world.

The Facebook investigation also sent a strong message to organizations operating online: the Internet is not a Wild West for privacy, and data protection authorities are watching.

Our involvement with Facebook continued over the years with further investigations.

We have also examined privacy issues on other social networking sites, including Nexopia, which specifically targets youth.

Cloud Computing

Business, individuals and even government are increasingly turning to cloud computing services, which can be a convenient way to store and manipulate large amounts of data without the usual headaches of managing an IT infrastructure.

However, cloud computing can also pose privacy risks, because of the sheer immensity of data being held on servers located in different parts of the world.

Recognizing this new trend towards cloud services and its significant privacy implications, we developed several educational materials aimed at various audiences. One fact sheet serves as a basic primer on cloud computing for a general audience. A second, more sophisticated

guidance document prepared in conjunction with our counterparts in Alberta and British Columbia, aims to help small- and medium-sized enterprises better understand cloud computing and their privacy responsibilities when they operate in the cloud.

Mobile Privacy

Modern mobile devices are carrying ever more personal data. When people are connected to the Internet, especially if they have enabled location-tracking functions, there is the growing risk of comprehensive individual surveillance.

In 2013, we collaborated with the Dutch Data Protection Authority in a precedent-setting investigation into the privacy practices of WhatsApp, a California-based developer of a cross-platform mobile messaging app. Our investigation into the company's mobile messaging platform turned up a number of risks to people's personal information.

WhatsApp undertook to address those deficiencies. For example, in partial response to our investigation, WhatsApp introduced encryption to its mobile messaging service and strengthened its authentication process in the latest version of its app.

In 2012, we joined our counterparts in British Columbia and Alberta to publish a guidance document for developers of mobile applications. The guidance provides advice about legal accountability, transparency and justifying the collection

of personal information. It also addresses the obligation to obtain meaningful consent for the collection of information, which is particularly tricky when users are flicking rapidly through privacy policies crammed onto tiny screens.

We have also launched a research project to examine privacy issues related to mobile payments. We expect that mobile payments will revolutionize the way Canadians pay for goods and services.

Google Wi-Fi

In 2010, an investigation by our Office found that Google contravened PIPEDA when it inappropriately collected personal information from unsecured wireless networks in neighbourhoods across the country.

Google cars photographing neighbourhoods for its Street View map service had also collected data transmitted over unprotected wireless networks installed in homes and businesses across Canada and around the world over a period of several years.

Google initially asserted that no personal information had been collected.

However, our technologists examined the data held by Google and discovered that, in fact, personal information – some of it highly sensitive – had been collected. It is likely that thousands of Canadians were affected by the incident.

We recommended that Google take steps to ensure that necessary procedures to protect privacy are duly followed before products are launched and to enhance privacy training for Google employees. Google implemented a number of remedial measures to address our concerns.

Biometrics

Another emerging technology with significant ramifications for privacy is biometrics. The term encompasses a range of techniques, devices and systems that enable machines to recognize people or confirm their identities by measuring and analyzing physical and behavioural attributes, including facial features, fingerprints, palm vein patterns, voice patterns, structures of the eye, and gait.

Biometric technologies, once largely the domain of law enforcement, are finding a home in the commercial and broader government sectors as well. Canada does not, however, have a policy on the use of biometrics, so there are no minimum standards for privacy, the mitigation of risk or public transparency.

In 2011, we published a primer on biometrics to help Canadians understand this rapidly developing field. Entitled *Data at Your Fingertips*, the document outlines the risks, as well as considerations that should guide organizations proposing to use biometric technologies.

Security Safeguards

Properly protecting personal information is a central component of good privacy. Not surprisingly, safeguards issues have featured prominently in many of our investigations and audits.

On the public sector side, for example, in 2010, we conducted audits that found the federal government's use of handheld communications devices and its practices for disposing surplus computers could put at risk the personal information of Canadians.

In 2012, the social networking site LinkedIn had nearly 6.5 million encrypted passwords stolen and posted online.

Given that LinkedIn has many users in Canada who might have been affected, our Office contacted LinkedIn with a view to examining the scope of the breach, and LinkedIn's breach preparedness and response.

We found that LinkedIn took immediate steps to escalate the breach to their senior management, notify users, and identify causes of the breach. These actions, and others that LinkedIn took in the wake of their breach, demonstrated an organizational commitment to accountability.

However, our discussions with LinkedIn also revealed some areas for improvement with respect to password management and network access management. In response, LinkedIn

said it would implement remedial measures to address our specific concerns.

WHAT IT MEANS FOR YOU

In a world of instant connectivity and e-everything, technology is everywhere. But it's generally in the background, and the more ubiquitous it is, the less we see it.

The trouble is that, the more we ignore the mechanics behind this modern miracle, the less likely we are to spot its shortcomings. And, more and more, the protection of privacy is becoming a serious challenge.

The work our Office has done in the field of Information Technology has helped decipher some of the complexity. We have identified where too much personal information is being collected or disclosed, without the meaningful consent of the affected individuals. We have pinpointed issues of transparency and information security.

Our Technology Analysis Branch and its laboratory have enabled us to explore the very frontiers of technology, garnering detailed knowledge about specific technologies with implications for privacy. We are now able to speak and understand the language of technology with private sector organizations and government institutions.

By consulting experts and focusing on emerging trends ahead of the curve, we have also bolstered our in-house expertise and reinforced our credibility among stakeholders.

This, in turn, has enabled us to issue well-received guidance and boost public awareness on a wide range of important issues.

LOOKING AHEAD

The reality is that the accelerating pace of technological change is creating new, complex and often unforeseen challenges to privacy.

We will continue to see cases involving information technologies – and also to see new technologies being used to enable initiatives that have privacy impacts in our other strategic priority areas.

The challenge will be to maintain our internal capacity to understand and assess the privacy implications of emerging information technologies by staying ahead of the curve, rather than falling behind.



PRIORITY



IDENTITY INTEGRITY AND PROTECTION

HOW IT BEGAN

When we first explored this priority, we thought about identity theft, where criminals steal personal information in order to commit fraud. We soon recognized, however, that the issue of identity integrity and protection is much broader. In fact, your identity is appropriated all day, every day, by all kinds of entities – for good and ill, as well as for reasons we may not be aware of, understand or agree with.

In the Information Age, people leave behind a trail when they browse online, post a

comment, use a credit or loyalty card, stroll past a surveillance camera, send an e-mail to a customer service department, or conduct any other sort of transaction.

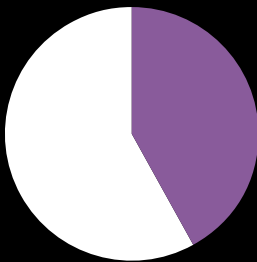
Your information bits are gathered up, cross-referenced and analyzed. With the right analytic software and know-how, organizations can create a highly detailed profile of you – their version of your identity.

This identity can be used for a multitude of purposes. It could be a ticket to VIP treatment at a store, or it could provoke a

BY THE NUMBERS

Polling by our Office reveals that only 42 percent of Canadians are confident that they understand how new technologies affect their privacy,

a significant drop
from a dozen
years earlier.



42%
understand

Survey of Canadians on Privacy-Related Issues, 2013

deluge of unwanted advertising. Governments can troll for signs of potential troublemakers. If your personal data gets into the wrong hands, you can fall prey to swindlers. Even ill-intentioned amateurs are appropriating other people's identities these days, leading to nasty impersonations and cyber bullying.

Our Office has worked to encourage private- and public-sector organizations to improve the way they protect personal information.

We have also encouraged individuals to improve their digital literacy in order to better manage their identities, particularly online.

We are concerned that people understand what can happen to their personal information in the digital world, and are better equipped to control it.

It all boils down to protecting the integrity of your identity.

WHAT WE OBSERVED

Our work under this strategic priority has highlighted a number of challenging trends.

Chief among them is the sheer volume of digital information that individuals leave behind in their day-to-day lives, often unwittingly.

Out on the streets, for instance, people's whereabouts and activities are routinely captured by surveillance cameras, cameras used to create street-view maps, or by other citizens wielding smart phone cameras.

As they browse the Internet, their online travels are tracked by numerous parties. Their personal data feeds into profiles that can be used to target them with advertising or for other purposes they know nothing about.

People are disclosing bits and pieces of who they are, whether they realize it or not. Posting comments or images online, using customer loyalty cards, or signalling their location with a GPS-enabled mobile device generates more data of interest to somebody.

People are also posting information about others. It could be a nice picture of a friend, or some nasty comments about an enemy. Cyber bullying – and its potentially devastating impacts – has become a significant concern in schools across the country.

This trend of individuals posting the personal information of others online poses a unique challenge for our Office, because our legislation is designed to address the privacy practices of commercial entities and the federal government – not those of individuals.

WHAT WE ACHIEVED

Given the rapid evolution of issues related to identity integrity, we felt it was important to thoroughly examine the landscape and seek the views of a wide range of experts in this area.

Our work in this area has helped us recognize and better understand the multiple ways in which our identities are shaped and managed.

In turn, this has allowed us to provide effective advice and guidance to both the private and public sectors on a wide range of issues, including, for example, government online identity management initiatives and online behavioural advertising.

As well, we have helped people to help themselves in this area by creating tools to enhance digital literacy.

Here are some examples of our work:

Consumer Privacy Consultations

In this evolving digital context, we recognized that Canadians need to feel confident that they can embrace new technologies and the e-economy, without forfeiting all control over their personal information. In 2010, therefore, we organized consumer privacy consultations to better understand the changing environment and to explore how best to protect privacy in this realm in the coming years.

One area of focus was the online tracking, profiling and targeting of consumers; the other, cloud computing, is described in the Information Technology and Privacy section of this document.

We wanted to learn more about certain industry practices, explore their privacy implications, and find out what privacy protections Canadians expect with respect to these practices.

Webcast public events held in Toronto, Montreal and Calgary pinpointed a range of challenges. For instance, participants highlighted a lack of transparency around online tracking, profiling and targeting,

The Rest of the Iceberg

This section highlights only a small selection of work we did within the scope of the Identity Integrity and Protection strategic priority. A comprehensive inventory of all our activities is available on our website. For example, you will find there descriptions of investigations involving identity integrity issues, links to digital literacy tools and fact sheets for individuals on issues such as reducing the risk of identity theft.

which makes it next to impossible to obtain the meaningful consent for the collection of personal information that is required under PIPEDA. There was also concern over the permanent retention of online data, prompting our Office to call on industry to address this issue with technical fixes.

We heard particular concerns about children online. Their personal information is especially vulnerable, and they cannot provide consent to its use. Children of all ages therefore need protection in the online universe.

The consultations gave us invaluable insights into the emerging challenges of the digital space, and where we need to be searching for solutions. They also laid the groundwork – and indeed created a framework – for a great deal of our work in identity integrity and protection. It also helped shape our views on the need for updates to PIPEDA.

Online Behavioural Advertising

Concerns raised at the consultations helped our Office develop a policy position and guidance about online behavioural advertising.

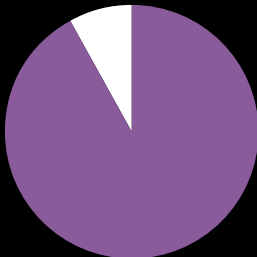
In online behavioural advertising, a third party who is typically unknown to you will track your web browsing behaviour, which is used to develop a digital profile of you. Based on your profile, organizations will infer your interests and target online advertisements or other shopping incentives at you.

We take the view that the information that is gathered for online behavioural advertising will generally constitute personal information under PIPEDA. Therefore, we argue that people must be properly informed that their online activities are being tracked, and must

BY THE NUMBERS

A survey by our Office found that a clear majority – 73 percent – of Canadians understand that their online activities can be tracked by government and commercial organizations. While fewer than four in 10 were concerned if the information was used for legitimate government or law-enforcement purposes, a majority drew the line at general surveillance by the state. Nearly three-quarters objected to companies using it to send spam.

A huge majority –
92 percent –
said companies
should have to ask
permission to track
people online.



92%

Survey of Canadians on Privacy-Related Issues, 2013

consent to that tracking. We acknowledged that a form of “opt-out” consent could be used in this case, provided certain requirements are met and certain practices are avoided.

Our *Privacy and Online Behavioural Advertising Guidelines and Policy Position* urge organizations to avoid tracking children, because they cannot give meaningful consent. It also calls for a reasonable way in which people can detect and control the practice. And it warns against the use of web bugs, web beacons, super cookies, pixel hacks, device fingerprinting or any new covert tracking technique invisible to users.

Digital Literacy

A key theme to emerge from our consumer privacy consultations was the need for privacy to be part of digital literacy or digital citizenship strategies. After all, threats to identity don’t just come from others; it is just as easy for people to make trouble for themselves and others. As many a politician and celebrity has discovered, it’s so much easier to fling an ill-conceived thought or image into cyberspace than to reel it back in again.

Such risks prompted us to develop fact sheets and other tools for Canadians of all ages. These include a general fact sheet on online privacy and others on online behavioural advertising, the use of cookies and cloud computing. We also developed tip sheets on protecting personal information on mobile devices, whether for personal or workplace use.

We sought out innovative ways to reach out to young people. Thus, for instance, we produced a graphic novel called *Social Smarts: Privacy, the Internet and You*. It aimed to help tweens and younger teens better understand and navigate privacy issues related to social networking, mobile devices and texting, and online gaming.

We also created youth presentation packages to show different school-age groups how technology can affect their privacy and how they can build secure online identities to keep their personal information safe.

Public Surveillance

Stroll down any city street or into a larger store, and chances are your image is being captured by video surveillance. Cameras are now in widespread use to control traffic infractions, enhance building security, aid law enforcement work, and a host of other purposes.

Camera-toting citizens are also apt to snap and share images of people in public places, especially when a newsworthy event breaks out. In conjunction with sophisticated systems to recognize patterns and faces, individuals and groups are under increasing watch.

Our view, however, is that being in a public place doesn't oblige you to surrender your right to privacy.

In 2006 we underscored this point in guidelines for the use of video surveillance in public places by law enforcement authorities. We followed up two years later with guidelines concerning overt video surveillance in the private sector, and covert video surveillance in the private sector in 2009.

In 2011, we investigated a complaint from a woman who complained that a Sobeys grocery store had collected her personal information without her knowledge and consent through in-store video cameras and then denied her access to her personal information, including a surveillance video recording. We concluded that Sobeys had collected the complainant's personal information without her knowledge and consent because there was inadequate signage about the surveillance cameras. Sobeys agreed to post decals on its storefronts and to place a visible, live monitor screen to alert shoppers to surveillance.

Our Office, along with three of our provincial counterparts, developed guidance on street-level imaging. We said it was important for companies to take steps to better protect privacy, for example, by using blurring technologies so that faces and licence plates can't be viewed and also by implementing responsive mechanisms to allow images where people may be identifiable to be blocked or taken down.



Government identity management initiatives

The federal government continues to make a concerted effort to be more strategic in its identity management initiatives. Since 2002, there has been an effort to create common identity credentials to access services across government that would be more cost-efficient and secure.

Recently, the federal government implemented both the GC Key, an authentication service that allows individuals to sign on to online enabled government programs and services using a username and password, and the Secure Key Concierge, an authentication service allowing individuals to sign on to online enabled government programs and services using their existing online banking login credentials. Both of these initiatives are part of the evolution of Treasury Board Secretariat's *Cyber Authentication Renewal Strategy*.

The OPC was extensively consulted during the planning phases of various identity credential services over the last 10 years and has reviewed over a dozen privacy impact assessments in this regard.

Thanks to the expertise developed through our work on the identity integrity strategic priority, we were able to respond in a strategic and consistent manner.

We were also consulted and provided advice during the drafting phase of the Standard

on Privacy and Web Analytics and its associated privacy impact assessment to provide guidance to federal government institutions on the manner in which they use web analytics. Treasury Board Secretariat addressed the majority of our Office's recommendations in the new Standard, particularly concerning the explicit prohibition on profiling individuals' web usage and timelines for retention and disposal of data.

WHAT IT MEANS FOR YOU

Our extensive and varied efforts under the Identity Integrity and Protection strategic priority – both in the public and private sectors – have contributed to our overall level of knowledge about the challenges and risks faced by Canadians.

At the same time, it has enabled us to work with organizations and individuals toward solutions.

It has, for instance, become clear that new technologies and business models are challenging the fair information principles.

In both the private and public sector, we see organizations collecting more and more personal information that must all be adequately safeguarded.

The private sector is using data analytics to track, profile and target customers, both online and off. Likewise, the federal government is leveraging these same powerful analytic tools in order to learn more about

Canadians and to meet pressing public needs. As well, we see an increasing number of public-private partnerships that involving the sharing of personal information.

In terms of the private sector, one of the fair information principles underlying PIPEDA requires organizations to obtain meaningful consent for the collection and use of their personal information. That is no simple task on a desktop computer; imagine the difficulty in the mobile space, with a tiny screen and only fleeting user attention.

To compound that challenge, people are flocking to these technologies, embracing apps of all kinds, and posting data about themselves and others – even if they don’t understand the privacy implications of their actions. But people are autonomous and their activities, in the main, fall outside the scope of personal information protection law.

We have focused on raising public awareness of privacy issues related to identity integrity through a variety of engaging and stimulating means – from social media and multimedia to public speakers series and graphic novels for young people.

But, of course, it’s not just up to individuals to protect themselves. And so we have also developed guidance, tools and innovative outreach initiatives to help government and private-sector organizations meet their privacy obligations. We also meet with organizations and departments to

learn more about current and emerging practices and to offer our comments on how Canadians’ personal information can be better protected.

We recognize that government and the private sector are always on the lookout for innovative ways to connect with citizens, customers and stakeholders. We would not wish to stand in the way of this impulse. But we do remind organizations that the foundation for innovation is user trust, and that is predicated on respect for the integrity of people’s identities.

LOOKING AHEAD

As Canadians continue to embrace new and smarter technologies, the risks to their personal information and the integrity of their identity will only escalate.

The idea that “people don’t care about privacy” simply isn’t true. The challenge lies in conveying information and ideas about an increasingly complex subject matter in a way that is accessible and easy to understand.

Organizations, meanwhile, must ensure they are investing appropriately in privacy and building privacy protections into their products and services – right from the start.

Finally, we believe that PIPEDA needs shoring up to ensure that the privacy rights of Canadians are properly protected in this digital era, and that their identity and the way they choose to present themselves to the world is fundamentally respected.



PRIORITY

GENETIC INFORMATION AND PRIVACY

HOW IT BEGAN

When it comes to personal information, it doesn't get more personal than your DNA.

While it's true that we are 99 per cent similar in terms of our genetic material, the unique 1 per cent sets each of us apart, making DNA the ultimate identifier.

What's more, your genetic information is not just a single factoid about you; it's a veritable library. It tells the story of your ancestry, your present, and potentially even your future.

All of this makes your genetic information extraordinarily precious to you – and profoundly tantalizing for so many others,

from police and medical researchers to insurance underwriters and your boss.

When we decided to select genetic information as one of our Office priorities, it wasn't because we were inundated with complaints or inquiries about the subject. We weren't.

We were, however, concerned about the potential future impact on privacy as the science of genetics was rapidly advancing.

And, as we began to really focus on the issues, our early concerns were borne out. The risks to privacy are already many, varied and vast. At the same time, the technologies to put

BY THE NUMBERS

A survey by our Office found that over half of Canadians say that if their doctor recommended genetic testing, they would be very concerned that

they may be asked to provide the results for non-health related purposes, such as obtaining insurance or applying for a job.

Survey of Canadians on Privacy-Related Issues, 2013

this sensitive information into the hands of individuals and organizations are becoming highly accessible.

We felt that genetics would be a game changer for privacy, and – somewhat to our dismay – we were more right than we ever anticipated.

WHAT WE OBSERVED

In the years since identifying genetic privacy as a priority, we have observed a number of important trends.

Over the last few years, we have seen an explosion in its use for a wide range of tests that are not predictive of future health.

Relatively inexpensive tests are readily available to determine paternity and provide answers about one's ancestry. Parents are using genetic testing in the hopes of finding clues about their child's potential to become a great athlete or musician. People also pay for nutritional genomics testing from companies that purport to identify the types of foods that best match their genetic makeup.

All of this has meant that an ever-growing amount of genetic information is in the hands of an expanding number of private companies – large and small, reputable and fly-by-night.

Employers and insurance companies have also identified genetic information as a tool for identifying who represents a higher risk of falling ill – and creating a cost burden for companies as a result.

Meanwhile, law enforcement agencies are also increasingly harnessing the power of genetic testing.

Police, immigration officials and others have been testing portable machines that can rapidly analyze DNA in the field for identification purposes.

This emerging DNA analysis tool – Rapid DNA – is another example of the interplay

between advances in genetic science and the increasing power, and falling costs, of information technologies.

Technological advances are also challenging the assumption that genetic information can be readily de-identified, allowing researchers to use the information anonymously.

Harvard University researchers recently demonstrated that they were able to re-identify more than 40 percent of a sample of anonymous volunteers taking part in a major DNA study being conducted by the university.

WHAT WE ACHIEVED

Back in 1995, our Office published a report, “Genetic Testing and Privacy,” that examined the then emerging science of genetic testing. The key challenge identified in that report was the need to determine how society could benefit from the potential of genetic science, without undermining individual autonomy and sense of self.

The advances of the years that have followed – the sequencing of the human genome and dramatic advances in genetic science – have made that challenge all the more pressing.

Our work under the umbrella of our genetic information strategic priority has put us in a much better position to take up that challenge.

Through the establishment of a genetic privacy working group, we have been able to identify priorities and build internal capacity and knowledge.

For example, in 2009, we organized a workshop with staff members and a number of external experts at which we discussed four issues: biobanking; the use of DNA for law enforcement purposes; direct-to-consumer testing and genetic discrimination. The workshop significantly increased the staff’s knowledge base and expertise to allow us to more meaningfully participate in and contribute to policy discussions regarding the governance and use of genetic information and it helped us establish our priorities.

As well, we have established important working relationships with centres of expertise such as Genome Canada and a number of academic experts that have allowed us to draw on specialized knowledge. We participated in a series of events on Genomics, Public Policy and Society, where we addressed issues of Genetics, Consent and Biobanks; Genetic Information and Insurance; as well as Online Direct-to-Consumer Genetic Testing.

All of these activities have strengthened our ability to support and inform the work of policy makers and Parliamentarians on a number of issues, in particular with respect to the use of DNA by law enforcement agencies.

As well, we have been able to translate our knowledge into information products for the general public.

Here are some examples of our work:

Genetic Testing

A 2010 study funded by our Office surveyed the privacy policies of companies which offer a wide range of genetic tests directly to consumers.

The study also provides Canadians with a three-page checklist of privacy questions to ask before signing up with a direct-to-consumer testing company.

Consumers who seek answers to the questions – through careful review of company privacy policies and direct contact with companies – will be able to make a more informed choice about sending their personal information and genetic samples to a company.

Our Office partnered with Genome Canada to organize a workshop series to foster a dialogue between policy makers and researchers on three issues: direct-to-consumer testing, genetic discrimination and the role of consent in biobank research. The workshops produced policy briefs designed to inform debate and discussion on these three issues.

Genetics and Insurance

Another rapidly evolving area of genetic privacy involves the potential use of genetic information by insurance companies.

Unlike in other countries such as the United States, there are no laws in Canada that specifically address the use of genetic information by insurance companies. Nor has any government here imposed a moratorium on the use of genetic information for insurance purposes, as in some European countries.

The Canadian Life and Health Insurance Association has adopted the position that although insurers would not require insurance applicants to undergo genetic testing, an insurer may request access to the results if an applicant has undergone genetic testing.

To help us better understand the industry and assess the Association's position, our Office commissioned two academic experts to look at the industry's argument that insurers need to have access to any available genetic information in order to accurately and fairly assess risks.

Their studies concluded that, at present and in the near future, a ban on the use of genetic information by the life and health insurance industry would not have a significant impact on insurers or on the efficient operation of insurance markets.

As a follow-up, we organized a roundtable discussion with various stakeholders.

The roundtable discussion, along with the research we commissioned, will help us

assess whether the collection and use of this information by insurers is necessary and whether a reasonable person would consider the collection and use appropriate in the circumstances.

To further public education about the predictive nature of genetics, we posted on our website a Q&A with University of Toronto professor of medicine Dr. Steve Scherer, director of the Centre for Applied Genomics at the Hospital for Sick Children.

Genetics and Law Enforcement

A particularly active area for our Office over the past few years has been the expanding use of genetic information by law enforcement agencies.

In Canada, the National DNA Data Bank was created in 2000, originally for the cataloguing of DNA from crime scenes and the DNA of anyone convicted of 37 very serious violent or sexual offences. However, the list of such “designated offences” has expanded to more than 265, greatly increasing the number of citizens whose supreme identifier is now on file with the RCMP.

We are an ex-officio member of the advisory committee for the National DNA Data Bank advisory committee, where we participate in overseeing the bank.

We commissioned research to compare the legal framework that regulates the banking of forensic DNA data in Canada with the United Kingdom, Australia, the Netherlands, the federal U.S. system and the states of California, Maryland and New York. The study found that, overall, Canadian data banking laws are either equally or more restrictive than the rules in those other jurisdictions.

In addition, the OPC has regularly commented on privacy issues related to the use of DNA for forensic purposes in speeches, as a member of the National DNA Data Bank advisory committee and in making submissions when Parliament carried out scheduled reviews of the enabling legislation.

There have been proposals to further expand the use of the National DNA Data Bank by allowing “familial” searching.

Suppose, for example, that police have a human DNA sample from the scene of a crime. A search through the National DNA Data Bank doesn’t find an exact match. So, instead police search for a near match, meaning a close blood relative likely to have a similar genetic profile.

From a privacy perspective, familial searching is troubling because it turns people into potential suspects not because of what they have done but simply because of their family relations.

In public speeches and in presentations to Parliamentary committees, our Office has marshalled arguments against familial searches on legal, ethical and operational grounds.

Similarly, the OPC has opposed proposals that the DNA of persons be included in the National DNA Data Bank as soon as they have been arrested.

Taking DNA upon arrest involves the retention of extremely sensitive personal information of individuals who may well be law-abiding citizens – in spite of being arrested.

Health Research

Our Office reviewed Privacy Impact Assessments related to a Statistics Canada longitudinal study that is exploring the relationship between disease risk factors and health status and identifying public health issues.

The Canadian Health Measures Survey involves the collection of thousands of biological samples, including samples of DNA.

We made several recommendations to increase the privacy of the voluntary participants. For example, we urged Statistics Canada to provide the participants with information on proposed research as it become available to allow them to reconfirm or withdraw their consent based on this new information. We also recommend

that participants be provided with a clear explanation of what happens to their samples if consent is withdrawn.

This example highlights the need to take privacy into consideration when conducting even the most socially beneficial scientific research.

WHAT IT MEANS FOR YOU

Highlighting genetic issues as a strategic priority for our Office has provided us with the opportunity to build our knowledge and adopt a forward-looking stance. This learning experience has allowed us to identify and begin to prepare for privacy issues of the future that will have very significant impacts on the lives of Canadians.

We are now in a much better position to assess the consequences for privacy and the implications for the fair information principles that underpin Canadian privacy legislation.

As well, we have developed an understanding of the international context of legislative initiatives to protect genetic information. We are also engaging with academics, government, the insurance industry and other stakeholders, to ensure we are staying abreast of rapidly changing developments.

All of these efforts have allowed us to provide more informed views to Parliamentarians and federal government policy makers. We have been able to raise the profile of privacy concerns in the area of genetics.

We believe that all of our activities under the rubric of this priority will help in our policy discussions and contribute to the continuing broad public debate about privacy and genetic information.

LOOKING AHEAD

Genetic science has already advanced at an astonishing rate and we are beginning to see the widespread use of genetic information in a number of contexts that raise privacy issues – insurance, employment and direct-to-consumer genetic tests, for example.

It is clear that we are still in the very early days of the use of genetic information. There is a need to carefully consider the potential privacy implications in order to develop sound principles to help mitigate those risks going forward.





THE ROAD AHEAD

The four selected priorities – public safety, information technology, identity integrity and genetic information – represent the most pressing privacy issues that have faced Canadians in recent years.

There is every reason to believe the privacy landscape will continue to evolve rapidly and we will see new and complex challenges related to these issues.

CONVERGENCE

Our focus has allowed us to identify some common threads between all the priorities that will undoubtedly continue to create challenges for privacy in the years ahead.

First, information technology is an enabler for the vast majority of the emerging privacy challenges of the 21st century.

While technologies can offer tremendous benefits, advancing technologies and analytic techniques will continue to pose clear challenges across all four priorities.

Indeed, the privacy risks related to some of those issues have intensified over the last several years as we have developed more advanced technologies and the cost of retaining information, as well as deploying certain technologies has dropped significantly.

As the real and potential uses of these technologies have become clearer, there has been increased interest in their use in both the public and private sectors.

Another common theme is that we increasingly see that the value of personal information to both businesses and

government lies in the information that is *derived* from the data we provide as consumers. This is one of the hallmarks of Big Data.

This will continue to raise issues in terms of the traditional approach to data protection.

One of the key characteristics of Big Data is “more” – collect more, use more. But that runs up against key privacy protections, specifically, that personal information can only be collected and used for a specific, identified purpose. How will consent work in such an environment?

The increasing focus on the use of personal data to attempt to make predictions – for example, with online behavioural advertising (what is this person likely to buy?); in law enforcement (who is a potential terrorist?); and with genetic testing (am I likely to develop a particular disease?)

From a privacy perspective, predictive capacities raise the possibility that decisions about us may be based on inaccurate or incomplete information or that organizations may know more about us than we know about ourselves.

INTERNATIONAL COOPERATION

In all four priority areas, we have also seen the vital importance of international collaboration and cooperation.

In a digital and interconnected world, privacy issues have become global.

People throughout the world rely on common information and communication technologies – we share information, videos and photos on a few highly popular social networking platforms; we play online games on the same platforms and we use the same search engines. Individuals increasingly buy goods and services from organizations based outside their own countries.

As a result of these trends, when one global company changes its privacy practices, or worse, when it experiences a privacy breach, millions of people worldwide can be affected.

Meanwhile, law enforcement and public safety issues have also been significantly been impacted by globalization – for example, with countries exchanging personal data regarding air travel and border control.

Global issues demand a global response, which is why our Office has worked hard to encourage cooperation by actively participating in a number of international organizations.

These include, for example, the Organisation for Economic Co-operation and Development (OECD), Asia-Pacific Economic Cooperation (APEC), the Global Privacy Enforcement Network, the *Association francophone des autorités de protection des données personnelles* and the International Organization for Standardization (ISO).

MODERN LEGISLATION

The rapidly changing nature of each priority has also highlighted the critical need for

privacy legislation to be regularly reviewed and updated to ensure it keeps up with emerging trends.

Our laws, our policies and our institutions have all been strained in the past decade given the pace of commercial evolution, governments' preoccupation with security and ever-changing public expectations.

For many, this has brought into question Canada's framework for the protection of personal information – in both the public and private sectors.

We believe it is time to modernize both the *Privacy Act* and PIPEDA to ensure they can meet the challenges of today – and the challenges that lie ahead.

Canadians deserve and expect to be protected by modern privacy laws that are relevant to the times.

A QUESTION OF ETHICS

All of these issues are profoundly important to the future of Canada. They raise questions not only about privacy rights, but moral and ethical issues as well. And they have implications for future generations.

Canadians have told us that privacy is a value they cherish. It is a critical element of a free society and there can be no real freedom without it. It is a cornerstone of our democracy.

This is why it is critical to be mindful of our choices.

The decisions we make today about public safety initiatives; about the technologies in our daily lives; and about the policies and legislation that protect our personal information will all have impacts long into the future.

The central question that governments, organizations and individuals need to ask themselves should no longer only be: Does privacy law allow this? But more importantly: *Should we be doing this?*

In other words: How do we define who we are? How do we relate to other individuals, organizations and governments? Essentially: *What kind of world do we want to live in?*

For more information, contact:

Tel: 1-800-282-1376

TTY/TDD: (613) 992-9190

priv.gc.ca

Follow us on Twitter: @PrivacyPrivee



Office of the
Privacy Commissioner
of Canada